FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

PERFIL DEL TRABAJO PREVIO LA OBTENCIÓN DEL TÍTULO DE:

MASTER EN REDES DE COMUNICACIONES

TEMA:

"PROPUESTA DE METODOLOGÍA PARA LA IMPLEMENTACIÓN DE PROYECTOS DE REDES – CASO DE ESTUDIO INSTITUCIÓN FINANCIERA LOCAL"

PABLO FERNANDO ERAZO GUERRA

Quito – Diciembre, 2016

AGRADECIMIENTOS

El más profundo agradecimiento a Dios por guiarme en cada momento de mi vida y bendecirme en la consecución de cada objetivo y meta propuesta; a mi amada esposa Mónica por ser la compañera ideal y por su actitud abnegada en el cuidado de nuestros hijos. A mis padres por su ejemplo y esfuerzo brindado, en especial a mi madre quien ha estado al pendiente de la culminación de mis objetivos.

DEDICATORIA

A mi esposa por su incondicional y abnegado apoyo brindado en todo momento y por su comprensión ante toda situación presentada.

A mis tesoros: Ariadne e Ian motores de mi vida, por quienes y para quienes junto con mi esposa efectuaremos toda actividad que permita brindarles los mejores ejemplos de valores, respeto y superación.

A mis padres por su amor y ejemplo brindado.

A mis queridos hermanos: Carla, Luis, Juan Carlos y mis sobrinitos: Nicole, Sebastián, Jorge Luis, Gabriel y Estefita.

A mis abuelitos: Raúl y Gloria por su sabiduría y consejos. Y en homenaje póstumo a mis abuelitos Manuel y Gladys.

A aquella institución que me permitió cumplir muchos sueños trazados y en donde se forjó e implementó este trabajo.

A la Pontificia Universidad Católica del Ecuador, en especial a todos los docentes que impartieron sus conocimientos durante mi paso por esta gran institución.

A todo lector que brinde su tiempo en la lectura de este trabajo que se ha desarrollado con mucho esfuerzo.

RESUMEN

En la actualidad, las empresas priman sus actividades enfocadas en la búsqueda de mejora continua, reducción de costos y mejora de sus procesos, políticas y procedimientos. En lo que respecta a nuevos productos y/o servicios; los ejecutan usualmente en base a metodologías existentes para ejecución de proyectos o lineamientos internos establecidos. Sin embargo, en lo que respecta a actividades que requieren el uso de redes y comunicaciones y si bien existen metodologías robustas para diseño de redes, se evidencia la carencia de un análisis y diseño apropiado generando inconvenientes al momento de la implementación de los mismos, muchos de ellos debido a la poca o nula documentación realizada y uso de metodologías en las actividades establecidas. Bajo esta problemática, el presente trabajo de investigación presenta una metodología para elaboración de proyectos de redes cuyo fin es brindar un marco de referencia para ejecución de los mismos estableciendo entregables que permitan obtener y mantener documentación actualizada de la red y que facilite la operación y mantenimiento de la misma. A su vez permita a la misma ser escalable ante nuevas funcionalidades que puedan ser requeridas.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

INTRODUCCIÓN

1.1 Introducción

El presente trabajo presenta una propuesta de metodología unificada para elaboración de proyectos de redes de comunicaciones en una institución financiera basada en metodologías exitosas para desarrollo de proyectos como son: PMI, Scrum; así como otras desarrolladas para el diseño de redes propuestas por el fabricante de tecnología Cisco Systems, tales como: Top – Down, y PPDIOO. Si bien el trabajo está enfocado en una institución financiera, este podrá ser aplicado en empresas e instituciones de todo tipo, pues su objetivo principal es ofrecer lineamientos sólidos para elaboración de proyectos que involucren uso de redes y tecnología.

La característica principal del presente trabajo es brindar un marco de referencia que sirva de apoyo al personal del área de redes y comunicaciones de las empresas ante la ejecución de proyectos, mantenimientos mayores o requerimientos específicos del negocio y que los mismos estén sustentados en documentación que sea útil para la institución.

De esta característica surge como una problemática pre existente, que en las instituciones suele llevarse a cabo la ejecución de requerimientos del negocio y proyectos sin tener una base en una metodología determinada que permita documentar cada una de las actividades, convirtiéndose así en un problema mayúsculo al momento de sustentarla ante auditorías internas y externas; lo propio ante pedidos de entidades gubernamentales de control que rigen bajo las instituciones financieras y dejando sin ejecución o solución la actividad o problema que en el inicio se quiso gestionar.

Es así que surge el interés de realizar un trabajo que sirva de aporte a los colaboradores del área de tecnología y demás relacionadas para el desarrollo de sus actividades cotidianas y que asimismo permita no sólo sustentar o documentar cada una de sus tareas; sino que sirva de fuente para realización de variables y métricas que permitan evaluar el desempeño de la red, elaboración de reportes gerenciales que apoyen y permitan justificar la necesidad de inversión en equipamiento y que a su vez apoye a la alta gerencia en el cumplimiento de los objetivos del negocio; exigiendo a su vez al ejecutor el realizar sus actividades en base a una metodología interna de uso estándar, que apoyará a futuro en el fortalecimiento de los procesos internos y mejora continua además de poder iniciar con establecimiento de estándares de procesos.

1.2 Justificación

En la actualidad las instituciones financieras y empresas en general se encuentran alineando sus procesos internos en base a estándares internacionales generalmente lineados a procesos de mejoramiento de la calidad, buenas prácticas, etc. con el fin de mantener la vanguardia ante un mercado globalizado y a la vez muy cambiante. Del mismo modo aumenta día tras día la necesidad de incorporar nuevos procesos que permitan la interacción del cliente o usuario final con la empresa mediante el uso de tecnologías eficientes que dependen mucho del uso de Internet; es así que surge la idea de acoplar una metodología que permita linear y normar los procesos y actividades a ser realizadas para ejecución de proyectos, ejecución de pedidos del negocio y actividades cotidianas que generen valor agregado al servicio que el área de tecnología brinda al negocio mediante la incorporación de lineamientos a seguir para la consecución de dichos objetivos. Dicha metodología se basa en definir y explotar las necesidades del negocio y acoplar las mismas bajo los diferentes documentos entregables que han de realizarse en las distintas fases del proyecto con énfasis en la infraestructura de la red existente (acoplando y

sumando servicios, es decir brindando escalabilidad), avalando en cada una de ellas lineamientos internos establecidos, cumplimiento de estándares existentes de redes, entre otros.

Por tanto, el presente proyecto se enfoca en realizar un estudio de diferentes metodologías propuestas para ejecución de proyectos, así como las metodologías existentes para diseño de redes para a continuación, que permitan presentar una propuesta para manejo de proyectos de redes, mantenimientos mayores y requerimientos específicos del negocio en una institución financiera, y finalmente aplicarla en un proyecto real de la institución referente.

La importancia de este proyecto es aportar a dicha institución una metodología que pueda ser utilizada internamente por el área de redes, y que a futuro pueda ser definida como estándar a seguir dentro del área de tecnología, siendo aplicable a su vez para otras sub áreas, con la ventaja de que adicionalmente y debido a su flexibilidad, la metodología desarrollada pueda ser utilizada por otras instituciones y empresas.

1.3 Antecedentes

Para el presente desarrollo, se ha tomado como referencia una entidad financiera local, en donde se tiene implementado a lo largo de su trayectoria mejoras en sus procesos internos. En lo que respecta al área de tecnología de dicha institución; se ha implementado como marco de trabajo a seguir para ejecución de proyectos, pedidos de negocio a MSF (Microsoft Solutions Framework), y en base a la misma se definieron documentos internos que han de ser ejecutados como estándar para ejecución de actividades realizadas por el área de tecnología.

Si bien MSF es muy aplicable en proyectos de desarrollo, proyectos de infraestructura y redes, los documentos internos definidos como estándar para uso del área de redes poseen entregables muy lineados al desarrollo de aplicaciones, resultando inútil en muchos de los casos el poder desarrollarlos. Esto conlleva a su vez problemas de documentación interna y lo propio

con la generación de información que es solicitada por entes de control tanto internos como externos.

Aunque se ha definido la presente problemática, no han existido trabajos internos que permitan atacar dicho problema. A su vez se ha identificado la necesidad de potencializar la información interna del diseño de red, permisos de firewall internos/externos, los mismos que debido a la no existencia de lineamientos a seguir simplemente no han sido generados o de haberlo sido, hoy se encuentran obsoletos e incompletos. La creación y/o actualización de los mismos nace bajo pedidos realizados en auditorías internas o externas más no como una actividad interna a ser ejecutada de manera continua. Respecto a los documentos existentes, los mismos no forman parte de la definición de fases de un proyecto.

Por parte del autor se propuso implementar una metodología de uso interno basado en el uso de metodologías existentes propuestas por Cisco Systems. De donde se pudo identificar como principal problema que las mismas se basan en el diseño de redes; es así que nace la necesidad de implementar una metodología interna en base a propuestas desarrolladas y existentes y acoplarla a la realidad de la institución siendo el objetivo principal del presente trabajo.

1.4 Objetivos

1.4.1 Objetivo General

- Realizar el análisis, estudio y comparación de las metodologías existentes para implementación de proyectos de redes propuesto por Cisco Systems (Top - Down Network Design, PPDIOO) y de proyectos en general: PMI, Scrum; que permita obtener lineamientos para ejecución de proyectos de redes

1.4.2 Objetivos Específicos

- Analizar las metodologías de Cisco (Top Down Network Design, PPDIOO) usadas en implementación de proyectos de redes
- Analizar metodologías para desarrollo de proyectos: PMI, Scrum
- Realizar un análisis comparativo de las metodologías: Top Down Network Design, PPDIOO, PMI, Scrum
- Presentar una propuesta aplicable al manejo de proyectos de redes, mantenimientos mayores o requerimientos específicos de negocio en una institución financiera que permita el establecer una gestión eficiente de red, con altos niveles de disponibilidad y seguridad
- Realizar un caso de estudio basado en un proyecto real propio de la institución bajo los lineamientos propuestos por el autor
- Establecer lineamientos para generación de entregables que permitan garantizar aspectos relacionados a brindar un buen diseño, implementación, operación y mantenimiento de la red que a su vez permitan definir actividades para las diferentes fases del proyecto junto a su respectiva validación de calidad, seguridad y disponibilidad
- Establecer lineamientos que aporten a la generación de diferentes métricas que permitan medir el desempeño de la red a fin de optimizar el uso de la misma
- Incorporar análisis de riesgos, aspectos de seguridad en el desarrollo de proyectos de redes, mantenimientos mayores o requerimientos específicos de la institución
- Alinear los entregables de las diferentes fases del proyecto hacia el cumplimiento de los objetivos del negocio, optimización de la red, exigencias de unidades

internas de control así como entidades externas y entes regulatorios, permitiendo así cumplir con normativas vigentes.

CAPÍTULO II

FUNDAMENTOS TEÓRICOS

2.1 Introducción

El presente capítulo realiza un acercamiento a los tópicos esenciales requeridos por el autor para conformar la metodología a ser propuesta. Es fundamental el mencionar y clarificar que cada una de las metodologías a continuación citadas poseen muchos tópicos que no necesariamente constarán en la presente, más brinda un detalle macro de cada una de ellas. El objetivo del presente capítulo es el brindar generalidades acerca de proyectos así como brindar una visión de cada una de las metodologías a ser revisadas. Los fundamentos expuestos servirán además a fin de fusionar los conceptos requeridos en la metodología propuesta por el autor.

2.2 Generalidades de metodología de proyectos

El presente tema realiza un breve acercamiento a la definición de proyectos en general; en lo que respecta a metodologías de proyectos así como un acercamiento a definiciones de metodologías de proyectos específicos de redes de comunicaciones. El fin es el poder establecer lineamientos bases bajo los cuales se ha de definir la metodología propuesta, brindando a su vez conceptos generales que son aplicados en las diferentes metodologías a ser revisadas en el presente capítulo. Las definiciones a continuación expuestas representan una síntesis elaborada por el autor bajo consideraciones expuestas por diferentes escritores; a su vez bajo definiciones generales acerca del tema.

2.2.1 Definición de proyecto

La palabra proyecto cuyo origen proviene del latín (proiectus) se define como un conjunto de actividades que poseen interrelación y que se encuentran coordinadas y alineadas en busca de un determinado objetivo o resultado. Para su ejecución forman siempre parte de un presupuesto y plazo establecido, adicional de un costo.

De acuerdo a la Guía PMBOK®"*se define como una tarea temporal que permite crear un producto, servicio o resultado único"* (Mulcahi, 2013, p21).

2.2.2 Elaboración de proyectos

Basa su esencia en el uso de una metodología cuyo objetivo contempla el reducir al máximo posible el nivel de incertidumbre y riesgos que pueden presentarse al buscar un objetivo determinado. Si bien con el uso de la misma puede minimizarse posibles impactos; ninguna metodología existente podrá asegurar el éxito del proyecto pues es imposible abarcar las diferentes variables y factores que puedan presentarse durante su ejecución. Bajo esta perspectiva la elaboración de proyectos de redes debe brindar lineamientos que aporten a la conclusión del objetivo planteado y garantizar cumpla los siguientes requisitos:

- Brindar escalabilidad
- Cumplir con normativas, estándares
- No afectar la continuidad del servicio

2.2.3 Dirección de proyectos

A lo largo de la vida, cada ser humano efectúa continuamente proyectos usualmente motivados por el cumplimiento de objetivos, solventar problemas, entre otros. Para ejecución de los mismos se suele analizar posibles alternativas, acudir en

busca de apoyo hasta finalmente tomar una decisión; misma que puede o no brindar el éxito esperado. A nivel personal existen proyectos que pueden ser ejecutados bajo una breve planificación, no obstante, en otros casos se requerirá una mayor profundidad en el análisis. Más; en lo que respecta al campo profesional; la toma de dichas decisiones requiere un nivel profundo de análisis pues las mismas pueden impactar incluso en la continuidad del negocio, pérdidas financieras, entre otros problemas y riesgos. La dirección de proyectos se define como la aplicación de conocimientos, aptitudes, herramientas y técnicas en las actividades; que conllevan a satisfacer necesidades y expectativas de una organización. Se enfoca principalmente en definir roles, actividades y niveles de autoridad en las actividades a realizarse así como proveer técnicas, herramientas y conocimiento para manejo de restricciones como son: costo, alcance, tiempo, calidad, recursos, satisfacción del cliente, riesgos y comunicaciones; de manera que permitan aumentar las probabilidades de éxito en la consecución del proyecto.

2.2.4 Antecedentes históricos

Como ha sido expuesto anteriormente, cada ser humano desarrolla proyectos a lo largo de su vida; es así que la ejecución de proyectos es un tema que nos han acompañado a lo largo de la historia; sin embargo y con fines de delimitar el uso de metodologías para ejecución de los mismos permite ya identificar y colocar un punto de partida cuyo inicio se remota a comienzos del siglo 20 y denota su despliegue entre los 90s y hasta la actualidad, en donde denota principalmente temas como calidad, globalización, sistemas productivos, gestión de procesos, de proyectos, mejora continua, reducción de tiempos, estandarización, uso de mejores prácticas, entre otros.

En la figura 1 se marca varios periodos respecto a la evolución de la Gestión de Proyectos:

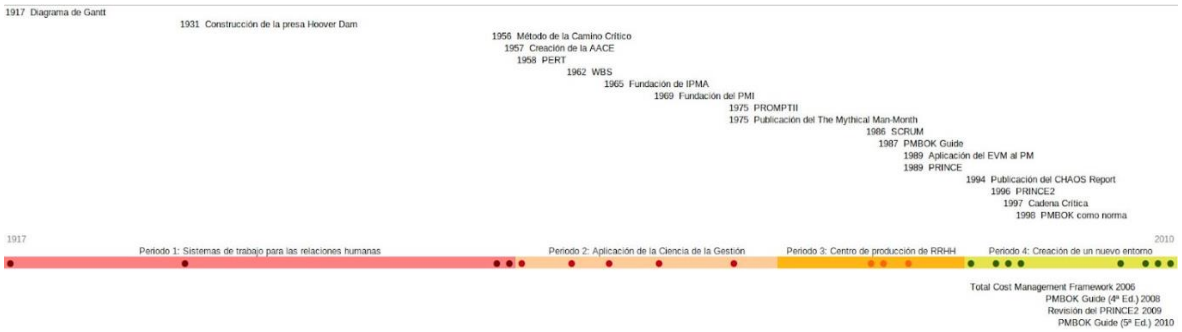

Figura 1. Evolución de la Gestión de Proyectos
Fuente: http://3.bp.blogspot.com/-2Hr8R5hushM/T7OvS0EjQGI/AAAAAAAAEcs/lVsN8Rs3sjw/s1600/Evolucion-de-la-gestion-de-proyectos+Ed2.1.jpg)

2.2.4.1 Periodo 1: Sistemas de trabajo para las relaciones humanas

- 1910 Taylorismo (gestión de procesos-reducción de tiempo)
- 1916 Fayol (funciones primarias de la gestión)
- 1917 Diagrama de Gantt
- 1918 Ford (mecanización de procesos)
- 1920 Toyota (5 porqué)
- 1930 Método Montecarlo
- 1930 Creación de ciclo PDCS (Plan, Do, Check, Act)
- 1931 Primer proyecto que usó Diagrama de Gantt
- 1940 Nakban, Sistemas de producción de Toyota y Lean Manufacturing
- 1941 Dupont (Principio de PARETO [80-20])

2.2.4.2 Periodo 2: Aplicación de la ciencia de Gestión

- 1956 Se crea el AACE (American Association of Cost Engineers)
- 1957 Método de ruta crítica CPM (Critical Path Method)

- 1958 Aparece PERT (Program Evaluation Review Technique)
- 1962 Aparece el concepto de estructura de desglose de trabajo EDT, conocido como WBS (Work Breakdown Structure)
- 1965 se funda IPMA (International Project Management Association)
- 1969 se funda PMI (Project Management Association)
- 1975 aparece PROMPTII

2.2.4.3 Periodo 3: Centro de producción de RRHH

- 1986 aparece SCRUM
- 1987 PMI publica la Guía PMBOK®
- 1989 se incorpora la Gestión de Valor Ganado EVM (Earned Value Management)

2.2.4.4 Periodo 4: Creación de un nuevo Entorno

- 1994 publicación del CHAOS REPORT
- 1996 aparece PRINCE como una evolución de PROMPTII
- 1998 ANSI reconoce a PMI como estándar
- 2006 AACE publica el marco para la gestión de costes
- 2009 se realiza una revisión profunda de PRINCE, conocida como PRINCE2
- 2010 se publica la actual versión de PMBOK®
- 2011 PMI promueve credencial tipo Agile, mostrando no estar cerrado a metodologías agiles
- 2013 Octava publicación del PMBOK® edición quinta

En cuanto a metodologías de proyectos de redes no se define una cronología definida; más se brinda a continuación una lista de las metodologías más conocidas:

- Top Down de Cisco

- Bottom Up de Cisco
- PPDIOO de Cisco
- Long Cormac
- James McCABE

2.2.5 Problemática existente en ejecución de proyectos de redes

"*Los profesionales de redes si bien poseen gran dominio acerca de conocimientos técnicos de la red que manejan; muy rara vez son capacitados en gestión de proyectos: Tema lamentable ya que la mayoría de problemas que enfrentan podrían ser mitigados con algunas habilidades y técnicas de proyectos, muy básicas",* (Schaffer, 2009).

Un proyecto de redes al igual que cualquier otro tipo de proyecto posee un objetivo, una línea de tiempo, un presupuesto y expectativas por parte de quienes se beneficiarán de la red una vez que esta se encuentre implementada. A su vez y al tratarse de una parte fundamental para continuidad de una determinada empresa su planeación debe ser muy rigurosa. Es así que se define al menos las siguientes bases a ser cumplidas para garantizar el éxito del proyecto. El mismo autor, expone ser requerido como mínimo el considerar los siguientes puntos:

- *"Identificar la triple limitación*
- *Definir el alcance y efectuar el acta de constitución del proyecto*
- *Definir cronograma*
- *Formalizar cambios de alcance*
- *Formalizar cierre del proyecto",* (Schaffer, 2009).

2.2.5.1 Identificar la triple limitación

Al igual que todo proyecto; se ve afectada directamente por la regla de las 3 limitaciones: **costo, tiempo y calidad,** ilustrado en la figura 2. Basado en el artículo del autor se define el siguiente ejemplo: "*Asumiendo que se trabaja en un proyecto cuyo fin es dotar de conectividad a una nueva sucursal, misma que deberá estar disponible en dos meses y para la cual se tiene un número de recursos asignados, resulta que desde la alta gerencia se solicita a las dos semanas de ejecutado el proyecto poder tener listo no en dos meses sino en un solo mes",* (Schaffer, 2009). Bajo este escenario, el administrador de red/ejecutor del proyecto deberá mediante el uso de la regla de las 3 limitaciones saber que requerirá colocar más recursos, tema que a su vez aumentará el costo inicial y que podrá tener incidencia en la calidad lo cual debe ser socializado con los diferentes intervinientes. Como se expone en el ejemplo anterior, es fundamental que el ejecutor tenga siempre en cuenta las tres limitaciones y las mismas deben ser socializadas con todo el equipo. El gestionar correctamente estas limitaciones permitirá tener éxito.

Figura 2. Triple restricción
Fuente: http://www.navegapolis.net/files/s/NST-001_01.pdf

2.2.5.2 Definir el alcance y crear el acta de constitución del proyecto

A fin que el proyecto de red no crezca descontroladamente deberá establecerse un alcance, el mismo que debe ser acordado desde el inicio entre todos los intervinientes y de sobre manera por el ejecutor del proyecto/administrador de la red y solicitante original. Es fundamental este alcance forme parte de un documento formal en donde se ha de definir el pedido específico. A su vez es esencial el formar el documento de acta de constitución del proyecto a fin de establecer allí los objetivos, entregables, responsabilidades, planes, consideraciones (riesgos, asunciones, restricciones) de manera que dicho documento autorice formalmente al proyecto y conste con requisitos iniciales que satisfacen las necesidades y expectativas de los interesados. Es fundamental estos documentos sean socializados, firmados y aprobados con todo interviniente del proyecto. Suele presentarse múltiples cambios durante la ejecución del proyecto por lo cual es esencial delimitar el alcance desde un inicio.

2.2.5.3 Cronograma

Una vez que se ha definido el alcance es esencial determinar un cronograma, el cual se ha de componerse por al menos: fecha de inicio, actividades de seguimiento, análisis de infraestructura existente, equipamiento requerido, planificación para configuración e instalación de equipos, conectividad, pruebas, aceptación del solicitante, documentaciones, implantación.

2.2.5.4 Cambios de alcance

Es usual que en proyectos se presenten posibles cambios de alcance; en lo que respecta a redes es de igual forma muy usual que se generen nuevos pedidos mientras el proyecto está siendo implementado. En este punto y si bien puede considerarse estos

posibles cambios, será requerido el ejecutar un análisis del desempeño de la red, tema que podría incurrir en nuevos costos y extensiones de tiempo. Bajo esta perspectiva, es fundamental el ejecutor del proyecto/administrador de la red formalice los cambios solicitados y ejecute los análisis correspondientes, considerando el impacto que pueda tener ante la disponibilidad y asegurando permita escalamiento.

2.2.5.5 Cierre del proyecto

Es fundamental que el ejecutor del proyecto/administrador de red realice 3 tareas esenciales previas al cierre del proyecto:

- Validar con el solicitante y asegurar que su solicitud fue cumplida. Formalizar con un documento de cierre, en donde exprese su aceptación
- Documentar; es esencial que todo elemento de la red este documentado, esto minimiza problemas
- Definir lecciones aprendidas, si bien un proyecto de redes muy rara vez termina según lo planeado es importante una vez concluido ejecutar una revisión sobre todo de las actividades que salieron mal y/o se desviaron a fin de documentar y evitar que los mismos errores vuelvan a generarse en el futuro.

2.2.6 Beneficios de la gestión de proyectos

Algunos beneficios asociados a la utilización de la gestión de proyecto son los siguientes:

- *"Los proyectos son necesarios para la evolución de la organización, y la gestión de proyecto es el conjunto de herramientas que permite que los proyectos alcancen sus criterios de éxito.*

- *La gestión de proyecto puede permitir a una organización producir una gama de productos más amplia con el mismo nivel de recursos",* (Wallace, 2014).

2.2.7 Desafíos de la gestión de proyectos

El autor expone adicionalmente respecto a los desafíos en la gestión de proyectos, que:

- *"Casi con seguridad, los proyectos competirán, por lo menos hasta cierto punto, con las unidades funcionales por recursos financieros y de otros tipos.*
- *La gestión de proyecto depende cada vez más de la utilización de técnicas y herramientas de planificación y control",* (Wallace, 2014).

2.2.8 Ciclos de Vida de Proyectos

Se define al ciclo de vida de un proyecto como "*el conjunto de fases por las que transcurre un proyecto desde que nace hasta que finaliza",* (Dr. Tapias, 2014, p4). Las fases varían de una a otra metodología. Si bien existen algunos ciclos, se exponen a continuación referencia a los dos más utilizados que serán estudiados en el siguiente capítulo.

2.2.8.1 Cascada

Se trata del modelo clásico a seguir dentro del ciclo de vida de fases del proyecto. Define una metodología rígida y secuencial en la cual se busca no iniciar una fase hasta haber concluido la anterior, se caracteriza por brindar mejor documentación, y al ser secuencial permite tener un mejor control de plazos y costos, se ilustra expuesto en la figura 3.

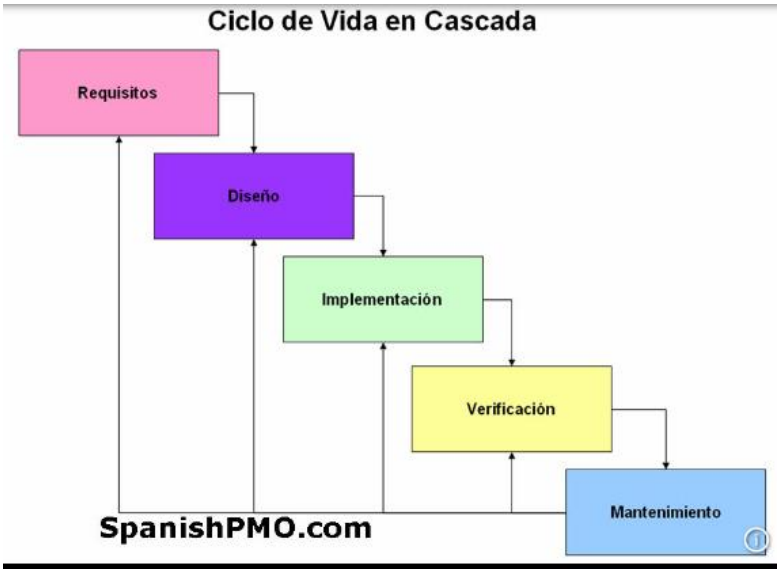

Figura 3. Ciclo de vida en cascada
Fuente: http://www.navegapolis.net/files/s/NST-001_01.pdf

2.2.8.2 Ágil

Se trata de un modelo flexible en donde se puede paralelizar actividades, muy usado en escenarios en donde se requiere brindar soluciones a requisitos de forma más rápida a su vez en escenarios en donde pueden presentarse cambios de alcance. Es más complejo el control de plazos y costos

Si bien existen otros tipos de ciclos de vida, se coloca los dos más importantes a los cuales se hará referencia a continuación.

2.2.9 Metodologías de Cisco

La creación de redes de Cisco se basa en tres métodos principales de diseño cuando se trata del diseño de red, de ellos; los dos primeros se relacionan con el objetivo de la red y el restante con su implementación global, siendo los tres métodos:

1. **Intelligent Information Network (IIN):** Este marco de trabajo permite adicionar inteligencia en la red. Esta inteligencia se extiende por las capas de la red y lo relaciona con el resto de la infraestructura de IT. El diseño de la red por ejemplo asegura que los

procesos del negocio pueden disponer de la información en el momento que les sea necesario.

2. **Service-Oriented Network Architecture (SONA):** Este marco de trabajo toma una estructura tradicional de red y ayuda a la misma a evolucionar hacia IIN. SONA asume que la red será unificada y que todo datos que se genere por ella atravesará una única arquitectura de red, es así que SONA provee gran escalabilidad al ser modular.
3. **Prepare, Plan, Design, Implement, Operate and Optimize (PPDIOO):** se trata de un ciclo de vida que Cisco usa para administración de redes. Su uso ayuda a aumentar la disponibilidad de la red y mejora la agilidad para realizar cambios en la misma.

Cada una de estas metodologías da lugar a la implementación de soluciones de red. De donde SONA provee una estructura a seguir, misma que permite y ayuda implementar IIN, mientras que PPDIOO es un modelo de implementación a seguir para implementar cualquier cambio en la red existente sea este pequeño o muy grande. En lo que respecta al presente estudio y el desarrollo del mismo, se considera solo a PPDIOO como metodología y ciclo de vida. Es así que se une la metodología Top Down misma que es usualmente usada para proyectos de diseño de red y que basa su esencia en el modelo de referencia OSI y a sus 7 capas, adhiriendo además limitaciones del negocio; referida como la octava capa, siendo su objetivo es asegurar el éxito en proyecto de diseño de red, acorde a los lineamientos y políticas de la empresa o negocio.

2.3 Metodología TOP DOWN DE CISCO

2.3.1 Origen

El desarrollo de la tecnología y la posibilidad de acceso remoto a la información conllevan a las empresas a adaptarse a estos cambios tecnológicos, permitiendo el acceso a sus datos desde lugares externos, sea que estos estén o no centralizados. Conlleva a su

vez a gestionar y mantener un cuidado exhaustivo en su diseño de red de manera que permita proveer escalabilidad y acceso sin perder de vista los objetivos de seguridad y propios del negocio, siendo el propósito principal de esta metodología el permitir cumplir con los objetivos del negocio sin importar la complejidad de las aplicaciones existentes mucho menos de las tecnologías requeridas, incluyendo si estas aplicaciones, tecnologías son requeridas sean accedidas desde o fuera de la empresa. A nivel macro esta metodología se centra en iniciar sus acciones desde la capa más alta de OSI para luego detallar capas inferiores de la misma, a su vez el poder adaptar la infraestructura física existente hacia las necesidades de las aplicaciones existentes. La realización de un diseño de red robusto deberá así englobar los objetivos del negocio y a su vez los objetivos técnicos, tema que impacta de sobre manera al realizar el diseño lógico previo a seleccionar los dispositivos de red físicos a ser usados. Cabe acotar que si la solución que espera el usuario final debe ser rápida o emergente podrá utilizarse Bottom-up; solo si los objetivos de negocio y técnicos están ya muy desarrollados e identificados.

Se recomienda en las obras consultadas para el presente desarrollo que para el caso de diseños de redes medianas o grandes dividirlas en porciones más pequeñas a fin de reducir posibles riesgos.

2.3.2 Beneficios

- Incorpora los requerimientos del negocio
- Provee al diseñador y al negocio una imagen clara del diseño de red a ser implementado

- Provee un diseño apropiado que satisface el requerimiento actual y es apto para futuras implementaciones

2.3.3 Desventajas

- Consume mucho más tiempo que otras implementaciones, por ejemplo frente a Bottom-up

A continuación se hace referencia a un ejemplo que permite brevemente evidenciar el aporte de top-Down en el diseño previo a una implementación de un requerimiento del negocio. El mismo detalla la "*implementación de una organización que requiere una red que pueda soportar telefonía IP a fin de reducir costos al no requerir dos redes separadas",* (Teare, 2008). Para obtener dicho resultado, la red existente debe ser compatible con la tecnología de VoIP, de donde como primer proceso de diseño a muy alto nivel se tendría algo similar a lo ilustrado en la figura 4:

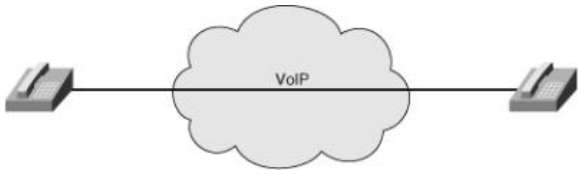

Figura 4. Primer diseño implementando Top-Down
Fuente: (Teare, 2008)

Como segundo paso y al realizar el análisis del caso se reconocería la necesidad de routers habilitados para IP además de haber brindado solución a un posible tema de retardo (delay) para los cuales se implementaría *"mecanismos de QoS a implementar en la red",* (Teare, 2008), tal y como se ilustra en la figura 5.

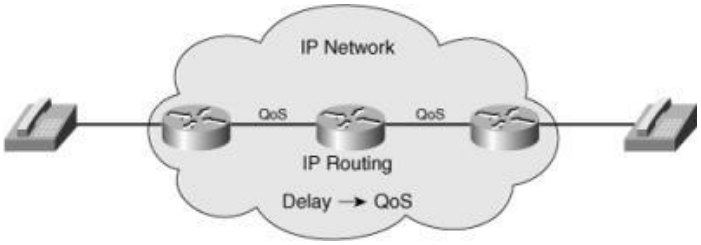

Figura 5. Análisis y validación de requerimientos Top-Down
Fuente: (Teare, 2008)

Como tercer paso y considerado como una optimización y bajo el análisis correspondiente; se identifica la necesidad de implementar funciones como monitoreo de llamadas y administración. En el caso del ejemplo citado "*se identifica la necesidad de implementar Cisco Unified Communications Manager a fin de gestionar y controlar las llamadas a realzarse mediante VoIP",* (Teare, 2008). Así se tendría un detalle final de la solución con in diagrama similar al provisto en la figura 6.

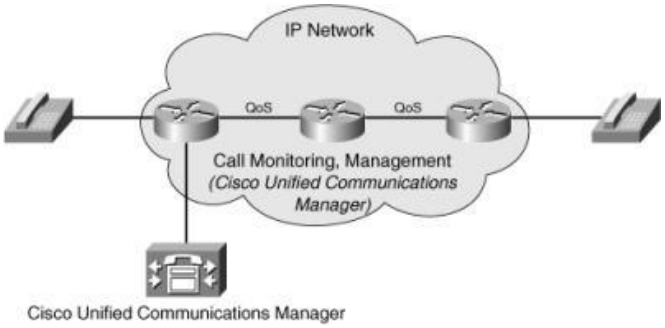

Figura 6. Optimización al requerimiento inicial aplicando Top-Down
Fuente: (Teare, 2008)

De existir factibilidad: es muy recomendable verificar un diseño previo a su implementación mediante un piloto, mejor si la misma pudiese ser ejecutada en una red de pre producción. Esta prueba de concepto seria así usada como la entrada previo a la implementación a ser ejecutada en la red de producción.

2.3.4 Lineamientos generales

- Se debe mantener una secuencia de arriba hacia – abajo (top - Down) durante toda las fases
- Mantener un total enfoque en: flujo de datos, tipo de datos a ser manejados, acceso a los datos
- Debe ejecutarse el diseño lógico previo a definir el modelo físico
- Las especificaciones se derivan de los requerimientos obtenidos del análisis ejecutado
- En redes medianas, grandes la modularidad es esencial para que el proyecto sea más manejable

2.3.5 Fases

La metodología Top-Down se basa en cuatro fases principales para obtener el diseño de red, las mismas son:

Fase de Análisis: Identificar las necesidades del cliente y sus objetivos

Efectuar entrevistas a usuarios finales y personal técnico con fines de comprender los objetivos del negocio así como los técnicos, comprende además el análisis de tráfico de la red actual con énfasis al tráfico de red futuro; valida además temas de calidad de servicio

Fase de diseño lógico: Diseñar la topología de la red

Valida además temas de seguridad de la red e identificar proveedores de servicio que pueden brindar soluciones de red a los requerimientos

Fase de diseño físico: tecnologías específicas y productos en base al diseño lógicos son seleccionados

La tarea de selección de proveedor de red debe ser complementada en esta fase

Fase de Pruebas, optimización y documentación del diseño de red: escribir y documentar un plan de pruebas, construir un prototipo o piloto, optimizar el diseño de red y documentar el diseño de red propuesto

El desarrollo de estas fases suele ser repetitivo ante lo cual es fundamental contar con la retro alimentación del usuario y monitoreo continuo. En la figura 7 se ilustra un detalle de las fases definidas para el ciclo de vida Top Down.

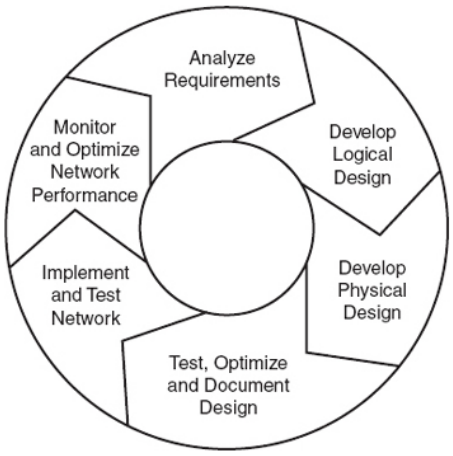

Figura 7. Ciclo de vida Top-Down
Fuente: (Oppenheimer, 2010)

2.3.5.1 Fase de Análisis: Identificar las necesidades del cliente y sus objetivos

Posee las siguientes actividades:

1. *"Análisis de objetivos del negocio*
    a. *Analizar objetivos del negocio*
    b. *Analizar restricciones del negocio*

   c. *Checklist de objetivos del negocio*

2. *Análisis de objetivos técnicos*

   a. *Checklist de objetivos técnicos*

3. *Validar la red existente (Análisis de estado de salud de la red)*

   a. *Validar el estado de Salud de la red*

   b. *Checklist de Estado de Salud de la red*

4. *Validar el flujo de Tráfico*

   a. *CheckList de validación del Flujo de Tráfico",* (Oppenheimer, 2010).

Análisis de objetivos del negocio

Analizar objetivos del negocio

Es fundamental poder comprender los objetivos y restricciones del negocio en la ejecución de un proyecto de red, mismo que ayuda al correcto desenvolvimiento del mismo, siendo un parámetro que ayuda de sobre manera al éxito del mismo. Previo a validar los objetivos del negocio es importante definir el tipo de industria en el cual está inmerso, así como identificar su nicho de mercado, productos, servicios, ventajas competitivas así como su relación con sus principales proveedores, de forma que el producto o servicio final del proyecto supla sus necesidades y brinde vanguardia dentro de la industria en la cual está inmerso. En la reunión con el solicitante/cliente es fundamental poder conocer el organigrama de la empresa, mismo que suele ayudar en el diseño en donde se pude definir si el mismo se ejecuta por departamentos, líneas de negocio, agencias remotas y/o otras opciones, además de permitir estructurar de mejor forma el flujo de tráfico a ser analizado. Finalmente permitirá conocer la jerarquía de

administración que permitirá conocer personas o áreas que pueden ayudar en la toma de decisiones.

Adicional a discutir acerca de los objetivos de negocio con el cliente es fundamental llegar a comprender cuales podrán ser los factores de criterio que permitirán medir el éxito del mismo así como determinar las posibles consecuencias de tener como resultado un fracaso.

Los temas fundamentales a ser definidos son los siguientes:

- Definir objetivos que deben ser necesariamente cumplidos
- Definir como el producto o servicio a entregar aportará en los objetivos económicos del negocio
- Definir qué tal visible es el proyecto a ser implementado ante la alta gerencia
- Definir en qué medida podría el comportamiento de la red interrumpir las operaciones del negocio
- Definir temas de seguridad y resiliencia
- Definir temas de continuidad del negocio

El diseñador de la red debe tener muy en cuenta detalles como: acceso remoto a los datos, virtualización, cumplimientos de procesos, políticas internas, externas (ejemplo: seguridad de datos: PCI). Evidenciando así la necesidad de brindar soluciones seguras, flexibles que ermita al usuario final trabajar de manera eficiente y segura sin importar el lugar desde el cual está conectado. Adicional y de existir los recursos necesarios debe brindar respuesta a temas de redundancias, disponibilidad 99.99% así como definición de continuidad de negocio.

Se expone a continuación algunos objetivos de negocio típicos:

- Aumentar los ingresos
- Expandirse a nuevos mercados
- Incrementar ventajas competitivas ante empresas del mismo segmento
- Reducir costos
- Incrementar productividad
- Ofrecer nuevos servicios al clientes, empleados
- Modernizar tecnologías obsoletas
- Evitar la interrupción del servicio

Adicional a la definición de objetivos es vital el definir el alcance del proyecto y enlazar este alcance en base al modelo de referencia OSI, ilustrado en la figura 8.

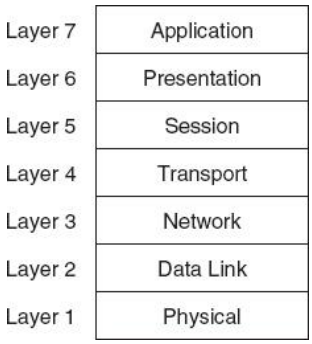

Figura 8. Modelo OSI
Fuente: (Oppenheimer, 2010)

Dentro de Top-Down se define el alcance de la red en base al alcance del diseño del proyecto de red, teniendo:

- **Segmento:** una red simple limitada por un switch o router en base a protocolos determinados de capa 1 o 2 como Fast Ethernet por ejemplo

- **LAN:** un conjunto de segmentos switcheados en base a protocolos de capa 2 como por ejemplo Fast Ethernet e inter switcheo troncal con IEEE 802.1Q
- **Red departamental:** consta de un conjunto de redes LAN distribuidas en una edificación, conectadas entre sí usualmente por una red de backbone.
- **Red de campus:** consta de múltiples edificios dentro de un área geográfica (unos pocos kilómetros) conectados de igual forma por una red de backbone.
- **Acceso remoto:** soluciones de red que dan soporte a usuarios individuales hacia la red.
- **WAN:** corresponde a una red geográficamente dispersa
- **Red inalámbrica:** red que usa el aire en lugar de cables como medio de transmisión
- **Red empresarial:** una red que se compone de campus, servicios de acceso remoto y de varias redes LAN o WAN, se la denomina como **internetwork**

Adicional a la identificación delos objetivos del negocio es esencial tener un enfoque sobre las aplicaciones que posee la empresa. El reporte a ser obtenido debe contemplar tanto las aplicaciones existentes como las nuevas a ser creadas, el detalle a ser recogido consta en la tabla 1:

Tabla 1. Levantamiento de aplicaciones

Nombre de la aplicación	Tipo de aplicación	Se trata de una nueva aplicación (Si o No)	Criticidad	Comentarios

Fuente: (Oppenheimer, 2010)

De donde;

Nombre de aplicación: usar el nombre con el cual el cliente la identifica, podría además llevar el nombre que posee en la industria la aplicación. Ejemplo (Lotus).

Tipo de aplicación: texto que describa la aplicación. Ejemplos: (correo electrónico, videoconferencia, educación en línea, control de inventarios, etc.).

Criticidad: definir el impacto de la aplicación dentro de la empresa, se recomienda usar 3 tipos:

- *"Extremadamente crítica 1*
- *Algo critica 2*
- *No critica 3",* (Oppenheimer, 2010).

Comentarios: podría incluir información relevante para el diseño de la red. Ejemplo (aplicación por ser migrada al Sitio alterno, aplicación por ser retirada de uso el año entrante, etc.).

Analizar restricciones del negocio

Así como se ha definido los objetivos del negocio es fundamental el analizar las restricciones del negocio que podrían afectar al diseño de red. Uno de los principales puntos a considerar es la validación de políticas y procesos internos así como identificar posibles gerentes o áreas que no están de acuerdo con la propuesta. Podría un proyecto ser técnicamente muy sólido y sin embargo no tener éxito a causa del no cumplimiento de estos temas. Es fundamental además poder identificar si las soluciones del proyecto causarán eliminación de trabajos manuales a su vez identificar si la propuesta en juego atenta ante alguna normativa gubernamental y/o legal. Cabe acotar y evidenciar que el

personal técnico suele no considerar estos temas, realizan su enfoque solamente en el aspecto técnico ignorando cualquier tema que no sea de esta índole.

Debe adicionalmente enfocarse en las limitaciones de presupuesto y de personal. Es de suma importancia verificar el presupuesto existente y saberlo administrar, a su vez es fundamental poder analizar el recurso humano interno pero sobre todo es fundamental involucrar en el proyecto a recursos que manejan el presupuesto (puede esto o no ser parte de TI) a fin de desarrollar planes de retorno de inversión, reducción de costos, mejora de productividad, expansión de mercado, mayor potencial de ingresos, etc.

Finalmente debe analizar las limitaciones de tiempo y bajo este parámetro analizar e identificar posibles factores que puedan influir en la salida planificada. Ejemplo (mal estado de instalaciones eléctricas, creación de puntos de datos).

Lista de verificación (CheckList) de objetivos del negocio

Es muy recomendable el realizar una lista de verificación de los temas que han sido validados, a su vez identificar en la misma temas pendientes que puedan presentarse. Se listan los principales puntos a ser considerados según metodología:

- Se ha investigado acerca de la industria donde se desempeña el cliente así como de sus competidores principales
- Se comprende la estructura corporativa del cliente
- Se ha recopilado una lista de objetivos del cliente en base al objetivo general del negocio
- Se han identificado operaciones de misión crítica
- Se comprende criterios de éxito del cliente así como de posible fallo

- Se ha definido el alcance del proyecto
- Se han identificado las aplicaciones de red del cliente
- Se ha identificado políticas y normativas
- Se cuenta y conoce el presupuesto para el proyecto
- Se cuenta con una fecha de salida requerida del proyecto
- Se ha verificado los conocimientos técnicos del personal

Análisis de objetivos técnicos

El análisis de objetivos técnicos puede ayudar a recomendar con confianza las tecnologías y/o equipos a ser provistos para una solución. La metodología define los siguientes objetivos técnicos y su respectivo significado:

Escalabilidad

Se refiere a la cantidad de crecimiento que un diseño de red puede soportar. Además que el mismo de poder adaptarse a lo ya existente y ser apto para incrementar en un periodo de tiempo.

Disponibilidad

Se refiere a la cantidad de tiempo que una red debe estar disponible, se representa con un porcentaje. Suele confundirse con fiabilidad, más este último posee relación con algunos temas como precisión, tasa de error, estabilidad.

Desempeño de la red

Este objetivo técnico tiene que ver con varios criterios de aceptación de rendimiento como son: retardo (delay), rendimiento (throughput), tiempo de respuesta, entre otros. A continuación una lista de los principales parámetros de desempeño que se suele analizar:

- Capacidad (ancho de banda): usualmente referida en bps en los equipos
- Utilización: porcentaje del total de capacidad disponible que se tiene en uso
- Rendimiento (throughput): cantidad de datos sin errores que pueden ser transferidos entre nodos en una unidad de tiempo
- Latencia (Delay): tiempo que tarda un paquete en estar disponible en otra parte de la red
- Tiempo de respuesta: cantidad de tiempo resultante de una solicitud de un servicio de red y de una respuesta a dicha solicitud.

Seguridad

Se trata de uno de los objetivos que debe llevar más énfasis dentro del diseño de red y tiene como objetivo principal el no interferir con la capacidad de la empresa para realizar negocios. Es fundamental en este objetivo el poder identificar y analizar los recurso de red existentes y proceder a identificar los equipos que deben ser protegidos. Cabe mencionar que los activos de la red pueden incluir hardware, software, aplicaciones y datos: no solo equipos. Se trata de un tema muy crítico pues se juega la reputación de la empresa, su disponibilidad, etc.

Manejabilidad

Es fundamental el identificar objetivos en cuanto a la capacidad de administración de una red, suele para algunas empresas ser importante el uso de SNMP para poder monitorear sus equipos, más para otras puede no serlo.

Usabilidad (Facilidad de uso)

Se refiere a la facilidad de uso para que un usuario final de la red pueda acceder a la red u a sus servicios. Al definir este parámetro debe considerarse y acoplarse por

ejemplo con las políticas de seguridad, puesto que las mismas podrían causar impacto en este objetivo

Adaptabilidad

Debe garantizarse la adaptación a nuevas tecnologías y cambios, solo de esta forma se puede garantizar a su vez una buena disponibilidad.

Asequibilidad

Suele llamarse adicionalmente relación costo beneficio.

Lista de verificación (Checklist) de objetivos técnicos

Es fundamental el efectuar una lista de verificación de los objetivos técnicos a fin de determinar si se han cumplido los mismos además de tenerlos presentes para futuras fases. A continuación una lista típica de objetivos:

- Se ha documentado los planes del cliente para expansión de sitios, usuarios y servidores para los próximos dos años
- Se ha validado planes de migración hacia un centro de datos, sitio alterno
- Se ha documentado los objetivos de rendimiento de la red
- Se ha validado con el cliente los riesgos y requisitos de seguridad de la red
- Se ha actualizado la tabla de aplicaciones de red para incluir objetivos de técnicos

Como se ha mencionado anteriormente, es fundamental actualizar la tabla de aplicaciones en base a objetivos técnicos fundamentales. Como es ilustrado en la tabla 2, en donde se incluye parámetros de: costo de inactividad, tiempo de respuesta aceptable, por ejemplo:

Tabla 2. Levantamiento de aplicaciones -criticidad

Nombre de la aplicación	Tipo de aplicación	Se trata de una nueva aplicación (Si o No)	Criticidad	Comentarios	Costo de inactividad	Tiempo de respuesta aceptable

Fuente: (Oppenheimer, 2010)

Validar la red existente

El análisis de la red existente del cliente (en caso de aplicar) puede ayudar mucho a entender la cultura del mismo así como a identificar el estado actual de la misma. Este entendimiento incluye el analizar su estructura de topología física actual, este análisis permitirá validar dispositivos y conexiones a ser reemplazadas, identificar y dar solución a problemas que permitan que la nueva red brinde inter operatividad entre la red existente y el diseño a ser incluido. En el caso de tratarse de un diseño desde cero asegura el comprender la estructura deseada por el solicitante y ayuda a recoger toda información requerida para cumplir sus expectativas.

En cuanto a redes existentes; es fundamental el realizar mapas de red e identificar la localización de los diferentes dispositivos, incluye este tema clarificar los nombres y direccionamiento de dichos dispositivos. Incluye además la validación del cableado, incluso analizar cimientos (en caso de redes inalámbricas) pues suele existir lugares de difícil acceso a la red inalámbrica; por temas de muros principalmente.

Para el desarrollo de mapas es recomendable apoyarse en herramientas como Tivoli de IBM, What's Up Gold de Ipswitch o LANsurveyor de Solar Winds o a su vez de herramientas manuales como Visio de Microsoft, lo fundamental en este punto es documentarlo. Cabe mencionar que es mucho mejor si se efectúan varios mapas que

permitan llegar a mayor detalle. El mapa de más alto nivel deberá proporcionan visibilidad a nivel de países, ciudades, provincias, agencias. En el caso de edificios y/o lugares donde consten equipos fundamentales para uso de toda la red debe establecerse un mapa a nivel de edificio (campus) que provea información acerca de: pisos, áreas y de haber el detalle a nivel de puestos de trabajo, detallar la ubicación donde están los servidores, routers, switches, firewalls, IDS, IPs, otros, (de aplicar).

Es de mucha ayuda el poder contar con un diagrama simplificado de bloque de la red, mismo que permite tener una impresión visual modular de las red, tal y como se muestra en la figura 9.

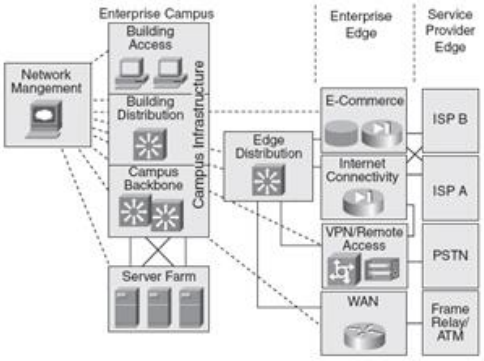

Figura 9. Diagrama de bloque
Fuente: (Oppenheimer, 2010)

En cuanto a nombres de equipos y direccionamiento se refiere; es importante contar con esta información a fin de poder definir el esquema de direccionamiento y validar el mismo con fines de mejora u optimización, a su vez y en el caso de nombres de equipos validar la existencia de un estándar y/o poder aplicarlo. Finalmente es necesario definir el cableado existente en la red, que permitirá conocer restricciones de distancia, en primera instancia se puede detallar a nivel muy general, como se ilustra en la figura 10.

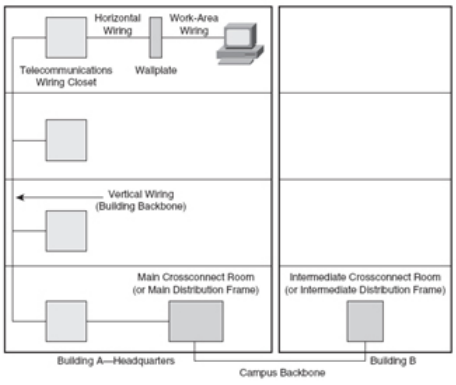

Figura 10. Ejemplo de cableado de una edificación
Fuente: (Oppenheimer, 2010)

Con la información levantada se puede proveer el detalle a nivel del cableado horizontal y vertical; así como el de conexión a filiales cercanas; de aplicar, para el caso se recomienda el uso de la tabla 3.

Tabla 3. Detalle del cableado

Nombre del edificio						
Ubicación del closet de telecomunicaciones						
Topología lógica del cableado (estructurado, estrella, bus, anillo, centralizada, distribuida, Estrella, árbol)						
Cableado vertical						
	Coaxial	**Fibra**	**STP**	**UTP Category 3**	**Category 5 o 6**	**Otro**
Eje vertical 1						
Eje vertical 2						
Eje vertical 1 *n*						
Cableado Horizontal						
	Coaxial	**Fibra**	**STP**	**UTP Category 3**	**Category 5 o 6**	**Otro**
Piso 1						
Piso 2						
Piso 3						
Piso *n*						
Cableado del área de trabajo						
	Coaxial	**Fibra**	**STP**	**UTP Category 3**	**Category 5 o 6**	**Otro**
Piso 1						
Piso 2						
Piso 3						
Piso *n*						

Fuente: (Oppenheimer, 2010)

Mientras se verifica el cableado es fundamental identificar a su vez objetos u entornos que puedan afectar al cableado: equipos que puedan emitir interferencia electromagnética, muros entre áreas. Debe identificarse adicionalmente lugares de difícil acceso, lugares propensos a error humano. En el caso de validaciones para redes inalámbricas es importante documentar obstáculos, áreas con fugas de agua; detalles y temas adicionales constan en estándares existentes.

Validar el estado de salud de la red existente

- Validar auto negociación de puertos especialmente entre equipos de diferentes proveedores, de ser el caso configurarlo de forma manual. En equipos Cisco ayudará en este tema el uso de comandos como **show port, show interface** validando el número y tipo de error
- Validar el MTU configurado en clientes y servidores y el existente entre routers
- Validar el estado de salud de los dispositivos. Es fundamental poder validar el uso de CPU del equipo, status de buffers, temperatura, voltaje de los equipos, es decir a medida de la posibilidad del equipo del vendedor; poder validar la información por el disponible.

Lista de verificación (Checklist) de salud de la red

- Documentar la topología física y lógica existente y/o validar que la información provista este actualizada
- Documentar nombres y direccionamiento de los dispositivos
- Validar que el cableado existente este correctamente estructurado y etiquetado

- Validar que el cableado de red haya sido probado y certificado
- Validar que los objetivos del cliente cumplas normas de disponibilidad y seguridad
- Validar status de equipos, según información disponible del fabricante

Validar el flujo de tráfico

Este punto hace referencia a técnicas que permiten caracterizar el flujo y volumen de tráfico y comportamiento de los protocolos. Al igual que en el caso de verificación de la red existente este centra su objetivo en temas de tráfico exclusivamente y en el caso de nuevos diseños describe los requisitos de flujo de tráfico a ser considerados. Para poder caracterizar el flujo de tráfico es importante identificar los orígenes y destinos a ser analizados.

Lista de verificación (Checklist) de flujo de trafico

- Estimar requerimientos de ancho de banda para cada aplicación
- Categorizar requerimiento de calidad de servicio para cada aplicación

2.3.5.2 Fase de diseño lógico: Diseñar la topología de la red

Esta fase se compone de las siguientes actividades:

1. *"Diseño de topología de red*
2. *Selección de protocolos de switching y de routing*
3. *Desarrollo de estrategias de seguridad de la red*
4. *Desarrollos de estrategias de administración de red",* (Oppenheimer, 2010).

Diseño de la topología de red

Se define como topología a un mapa de un conjunto de redes que indica segmentos de red, puntos de interconexión y comunidades de usuarios que brinda un modelo de alto nivel de la red, es además el paso más importante de la metodología top-Down. Previo a cumplir objetivos de un cliente en temas de escalabilidad y seguridad y previo elegir equipos esta actividad debe ser desarrollada.

Diseño de red jerárquico

El diseño jerárquico tiene como objetivo recomendar una topología de red que consta de muchos componentes relacionados y ejecutarlo mediante división de capas de manera que se torne una actividad más fácil, dichas capas se ilustran en la figura 10 y son las siguientes:

- **Capa núcleo (core):** constan routers de alta gama y switches que proveen alta disponibilidad y rendimiento. Su rol es proveer trasporte óptimo de datos entre sitios.
- **Capa distribución:** constan routers y switches en donde se implementan políticas (s se tratas de redes pequeñas y/o medianas) la capa de núcleo y distribución suelen estar combinadas. Su rol es conectar servicios de red a la capa de acceso e implementar políticas de seguridad, tráfico y ruteo
- **Capa acceso:** conecta a los usuarios a través de switches de gama baja y/o por medio de puntos de acceso inalámbrico. Su rol es proveer conectividad a usuarios finales.

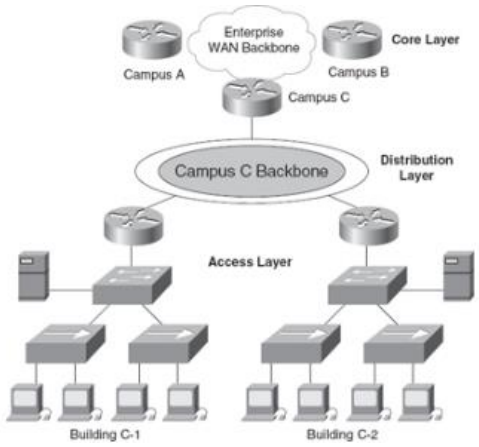

Figura 10. Topología jerárquica
Fuente: (Oppenheimer, 2010)

Una forma de determinar si la topología posee ya los ítems adecuados se identifica por los siguientes lineamientos:

- Cuando se torna muy fácil el entender como añadir un nuevo piso, enlace WAN, edificio, sitio remoto, etc.
- Cuando un determinado cambio causa solo cambios locales a los dispositivos conectados
- Cuando la red puede duplicar o triplicar su tamaño sin grandes cambios de diseño

Diseño de red redundante

Permite proveer mayor disponibilidad de la red, su fin es evitar puntos únicos de fallo en la red. Se suele brindar redundancia a nivel local así como a nivel de borde en donde el fin es asegurar una lata disponibilidad de servicios externos como Internet, acceso por VPN. Cabe mencionar que todo servicio de redundancia trae consigo altos costos ante lo cual es preciso determinar si los mismos constan dentro de los objetivos técnicos y de negocio de la empresa.

Selección de protocolos de switching y routing

Es fundamental identificar los protocolos a ser usados en la red y en base a estos determinar el tipo de switch o router a ser adquirido. Por ejemplo en el caso de uso de VLAN es fundamental verificar si serán implementadas a fin de adquirir equipos que la soporten. En lo que respecta a los routers es fundamental poder conocer los protocolos de ruteo a ser usados y en base a esto poder a la adquisición del equipo que cumpla las necesidades requeridas.

Desarrollo de estrategias de seguridad de red

Se trata de uno de los elementos más críticos al diseñar una red, considerando se debe proveer una red segura pero a su vez que deberá ser de fácil uso y alto rendimiento.

Diseño de seguridad de la red

El diseño de seguridad al igual que el diseño de red como tal, requiere poder estructurarse en varios pasos a ser validados, de tal forma que se pueda llegar a obtener una estrategia efectiva, se considera los siguientes pasos (algunos de ellos ya considerados en pasos anteriores):

1. **Identificar los activos de la red**
2. **Analizar riesgos de seguridad** (pueden ser generados por usuarios internos o por atacantes externos)
3. **Analizar requisitos de seguridad** (abarca objetivos específicos del usuario final pero suelen referirse a proteger la confidencialidad de los datos brindando acceso autorizado a información sensible, integridad de los datos de tal forma que solo usuarios autorizados pueden modificarlos y brindar

disponibilidad de los datos, de tal forma que el usuario solicitante y autorizado pueda acceder a ellos cuando le sea requerido

4. **Desarrollar un plan de seguridad** es un documento a alto nivel en el cual se detalla actividades a ejecutar para cumplir con los requisitos de seguridad, el mismo detalla tiempo, personas y recursos que son necesarios para poder crear una política de seguridad
5. **Definir una política de seguridad** establece lineamientos a ser cumplidos por los usuarios, administradores y personal técnico para proteger los activos tecnológicos. Es un documento vivo que requiere ser actualizado. Debe incluir lineamientos para acceso a la red, definir responsabilidad de los usuarios, definiciones de autenticación
6. **Desarrollar procedimientos para la aplicación de las políticas de seguridad** los procedimientos forman parte de una política, es aquí donde se establece por ejemplo temas de configuración, inicio de sesión, mantenimiento, majeño de incidentes, entre otros
7. **Desarrollar una estrategia de implementación técnica**
8. **Lograr la aceptación por parte de los usuarios, administradores y personal técnico** debe esta información ser divulgada a todo usuario y formalmente aceptada
9. **Capacitar usuarios, administradores y personal técnico**
10. **Implementar los procedimientos de estrategia y técnicas de seguridad**
11. **Realizar pruebas de seguridad y actualizar si se detecta algún problema**
12. **Mantener la seguridad**.

Como se evidencia en los últimos puntos expuestos en líneas anteriores (9-12) es esencial el mantener informado al usuario final y capacitarlo en estos temas, a su vez el definir políticas de estrategia, validarlas y tenerlas actualizadas y mucho más importante es el mantener los lineamientos de seguridad establecidos en todo momento.

Mecanismos de Seguridad

Seguridad física

Se refiere a la limitación de acceso a recursos de red, mismos que deben poseer protección detrás de una puerta cerrada y colocada en lugares protegidos en lo posible a desastres naturales, error humano.

Autenticación

Se refiere al acceso a servicios de red, generalmente a través de un usuario y clave mas también se refiere por ejemplo a accesos con biométrico, acceso mediante tarjeta de seguridad. Se recomienda en este punto poseer y/o implementar sistemas de autenticación de dos factores.

Autorización

Complementario a la autenticación, la autorización define los niveles de permisos que posee un usuario sobre el servicio de red requerido. Sobre este punto es recomendable el uso del principio de mínimo privilegio.

Auditoria

Para poder determinar incidentes de seguridad debe implementase mecanismos que permitan guardar registros de autenticación de los usuarios.

Cifrado de datos

Se debe implementar procesos de cifrado a fin de brindar confidencialidad de los datos que viajan por la red

Filtrado de paquetes

El filtrado de paquetes puede ser incorporado en routers, firewalls a fin de aceptar o denegar paquetes de direcciones o servicios particulares. La implementación de los mismos permite proteger los recursos de red y evitar ataques de denegación de servicio. Suelen implementase por medio de políticas (listas de acceso) en las cuales se especifica paquetes a ser aceptados y denegar lo demás o negar ciertos paquetes y permitir lo demás

Firewalls

Implementa políticas de seguridad entre dos o más redes, usualmente usado para proteger la red empresarial de Internet.

Desarrollo de estrategias de administración de red

Diseño de administración de red

Un buen diseño de administración de red puede ayudar a una organización a lograr los objetivos de disponibilidad, rendimiento y seguridad. Los procesos eficaces de gestión de red pueden ayudar a una medida de la organización cómo se están cumpliendo los objetivos de diseño así y ajustar los parámetros de red si no se cumplen estos objetivos. Suele implementarse herramientas de administración de red que soportan protocolos como SNMP a fin de obtener un monitoreo visual de la red.

2.3.5.3 Fase de diseño físico: tecnologías específicas y productos en base al diseño lógico son seleccionados

El diseño de red físico se basa en la selección de equipos en base a los requerimientos establecidos durante el diseño lógico. Un buen diseño inicia por la implementación de los equipos a nivel LAN para luego implementar soluciones WAN y accesos remotos.

Criterios para selección de dispositivos de red

Se define los siguientes criterios para selección de dispositivos de red:

a. *"Número de puertos, Velocidad de procesamiento, Cantidad de memoria, Cantidad de latencia introducida cuando el dispositivo transmite datos, Rendimiento en paquetes por segundo, Técnicas de ingreso / egreso de colas y buffers, tecnologías LAN y WAN compatibles, Detección automática de la velocidad, Auto detección de operación half o full dúplex, Cableado soportado, Facilidad de configuración, Capacidad de administración (SNMP), Costo, Actualizaciones de software, Soporte para funciones de QoS, Reputación y la viabilidad del proveedor", (*Oppenheimer, 2010),

Presentándose consideraciones propias por cada tipo de dispositivo (ejemplo switches, routers, etc.).

2.3.5.4 Fase de Pruebas, optimización y documentación del diseño de red: escribir y documentar un plan de pruebas, construir un prototipo o piloto, optimizar el diseño de red y documentar el diseño de red propuesto

En esta fase puede implementar un piloto o ejecutar un prototipo por medio de herramientas existentes para el efecto, misma que permitirá predecir el comportamiento esperado de la red. Suele existir soporte de algunos fabricantes para implementar un piloto en un laboratorio o como fue mencionado poder ejecutarlo por medio de una herramienta que permita simular la red esperada. Durante la ejecución de estas validaciones debe documentarse y analizárselos resultados obtenidos con fines de poder implementar mejoras u optimizaciones, entre ellas puede destacarse por ejemplo técnicas de switcheo.

El último paso de la metodología Top-Down define el documentar el diseño de red propuesto. Dentro de la metodología se define el documento RFP (Request for proposal – Solicitud de una propuesta) que se trata de un documento que enumera los requisitos de diseño del cliente y los tipos de soluciones de un diseño de red. Suelen poseer distintos formatos pero en general brindan atención a los siguientes temas:

- Objetivos del negocio para el proyecto
- Alcance del proyecto
- Información existente de la red y aplicaciones existentes
- Información sobre nuevas aplicaciones a ser implementadas
- Requisitos técnicos
- Requerimientos de garantía de los productos
- Restricciones ambientales o arquitectónicas que pueden afectar la solución
- Requisitos de capacitación o soporte
- Calendario preliminar con hitos y resultados
- Términos y condiciones contractuales legales

En casos de propuestas suele detallarse además:

- Topología de red para el nuevo diseño
- Información sobre protocolos, tecnologías y productos que forman el diseño
- Plan de implantación
- Plan de capacitación
- Información sobre soporte y servicio
- Precios y formas de pago
- Calificaciones del proveedor
- Recomendaciones de otros clientes con implementaciones similares
- Términos legales

2.4 Metodología PPDIOO DE CISCO

2.4.1 Origen

La metodología PPDIOO posee su origen bajo los lineamientos propuestos en el ciclo de vida PPDIOO que usa Cisco para administración de red. El seguimiento de este ciclo de vida propuesto ayuda a cumplir objetivos trazados como son la disminución del costo total de administración de la red y aumento de disponibilidad de la red a su vez mejora en agilidad para implementación de cambios en la estructura de la red. El ciclo de vida así puede ser útil para implementación de nuevas redes así como para actualizaciones en redes existentes. Los elementos que conforman el ciclo de vida forman un círculo sin fin puesto que por ejemplo el paso de optimización conlleva a realizar actividades como identificar cambios, validar en la infraestructura existente; misma que conllevarían a iniciar desde el paso de preparación**.** A

continuación se presenta una ilustración en la figura 11 en donde constan las fases de esta metodología.

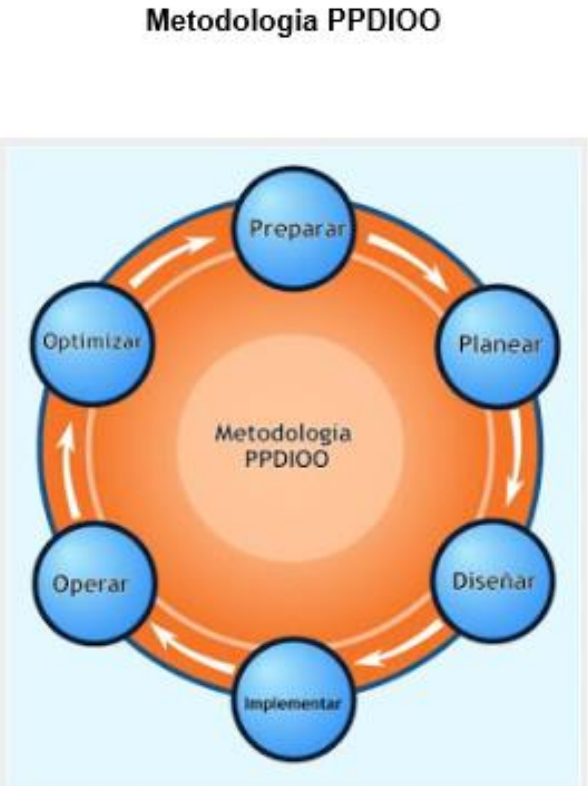

Figura 11. Ciclo de vida PPDIOO
Fuente: http://redplataformabibliotecakatherinebrech.blogspot.com/2012/10/normal-0-21-false-false-false-es-x-none_27.html

2.4.2 Beneficios de PPDIOO

- **Disminución de costo de propiedad** al realizarse validaciones de: requerimientos de tecnología, planeación de cambios en la infraestructura y determinación de requerimientos de recursos. Además al contemplar y alinearse con los requisitos técnicos y objetivos de negocio. Y finalmente al mejorar la eficiencia de red y del personal de apoyo y disminución en costos operativos

- **Aumento de disponibilidad de la red** al proporcionar un diseño solido de la red que posee altas consideraciones de seguridad que soportan el diseño propuesto. Además de ejecutar pruebas piloto o prototipos previo a la implementación en producción
- **Agilidad de los negocios** estableciendo requisitos de negocio, integrando requisitos técnicos y objetivos de negocio en un diseño detallado y mediante un alto dominio de experiencia en la configuración, instalación e integración de los componentes del sistema además de existencia de mejora continua
- **Mayor velocidad de acceso a aplicaciones y servicios** mediante análisis profundo de objetivos técnicos y análisis de equipos y tecnologías a ser implementados que soportan los servicios de red actuales y previstos. Amento de disponibilidad de la red y de las aplicaciones que se ejecutan sobre ella

2.4.3 Fases del ciclo de vida PPDIOO

PPDIOO conforma su acrónimo con cada primera letra (tomado del inglés) de la fase que la compone, siendo:

P (Prepare) Fase de Preparación involucra temas de presupuesto, estrategia de red

P (Plan) Fase de Planeación involucra evaluación de la red, análisis de deficiencias

D (Design) Fase de Diseño involucra el diseño de la solución (productos, servicios)

I (Implement) Fase de Implementación involucra la puesta en marcha dela solución

O (Operate) Fase Operativa involucra el mantenimiento de la red

O (Optimize) Fase de Optimización involucra la administración proactiva de la red

Fase de Preparación

En términos generales en esta fase se crea un caso de negocio para establecer una justificación financiera para una estrategia de red. En la misma se establece lineamientos generales del proyecto e impacto ante el negocio. Usualmente el caso de negocio a ser implementado resuelve varios problemas, debilidades o deficiencias que son reportadas por los usuarios, definidos como requerimientos de cliente o usuario final. En lo que respecta a la estrategia de red es determinada en base a los objetivos de negocio. Finalmente se examina las tecnologías necesarias que soporten los requerimientos definidos.

La definición de requerimientos del cliente determina y documenta los siguientes puntos:

- **Servicios y aplicaciones de red** debe validarse las aplicaciones y servicios que actualmente son soportados por la red (en caso de existir) así como definir las aplicaciones y servicios a ser implementados.
- **Objetivos organizacionales:** dependiendo el tipo de organización se presentarán objetivos propios determinados, más en términos generales suelen ser referenciados en: reducción de costos, agregar productos basados en tecnologías de vanguardia, brindar nuevos servicios al usuario final, mantener una posición competitiva en el mercado, entre otros.
- **Restricciones organizacionales** así como se definen objetivos propios dentro de una organización; en la misma existen limitantes ya conocidas bajo las cuales el diseño debe ser desarrollado. Las restricciones generalmente se presentan principalmente por temas de presupuesto y tiempo, más pueden presentarse por temas de políticas internas, políticas externas (gubernamentales, legales)

- **Objetivos técnicos** deben ser alineados a los objetivos organizacionales pero desde la perspectiva técnica. Uno de los principales temas que debe cubrir es el modernizar tecnologías antiguas, simplificar la administración, reducir fallas de los equipos, proveer escalabilidad de la red

En lo que respecta a documentos entregables de esta fase se tiene:

- **Documento de requerimientos del cliente**
- **Arquitectura de estrategia de red**
- **Caso de negocio**

Fase de Planeación

En términos generales esta fase realiza una evaluación de la red actual orientado en el análisis de deficiencias contra buenas prácticas. Desde la perspectiva de proyecto en esta fase se define tareas, responsables, hitos y recursos que se ejecutarán durante el desarrollo del proyecto. De definirse en esta fase los riesgos potenciales así como validar los recursos con los cuales se cuenta incluyendo hardware, software así como personal técnico disponible. La evaluación de la red suele requerir el uso de herramientas de administración de red con fines de examinar la salud actual de la red y expone deficiencias a ser resueltas, la información recogida en esta fase es fundamental para selección de dispositivos requeridos. Para la ejecución de este análisis en equipos Cisco y de algunos fabricantes suele implementarse comandos que permiten obtener información útil para este fin, de igual forma existen herramientas que permiten obtener información, de donde es esencial el verificar:

- Segmentos Ethernet deben tener un porcentaje de utilización menor al 40%

- Validar que los segmentos adicionados a la red deben ser switcheados con switches (de preferencia administrables), en lo posible eliminar hubs
- Enlaces WAN deben tener utilización menor al 70%
- Tiempo de respuesta entre sistemas locales debe ser más rápido que 100 ms
- No debe existir altos umbrales de tráfico broadcast o multicast
- La tasa de colisiones debe ser menor que 0.1%
- Uso de CPU debe ser menor al 75%
- Colas deben ser menor que 100 para salida y 50 para entrada

En lo que respecta a entregables de esta fase se tiene:

- **Documento de evaluación arquitectónica actual**
- **Documento de alto nivel (HLD)**
- **Prueba de concepto (POC)**
- **Documento de capacidad de la red (Capacity Planning)**

Fase de Diseño

En términos generales se inicia con el diseño de red en base a la información obtenida en fases anteriores. El plan del proyecto se actualiza con información ya más granular y específica, misma que servirá para la implementación. Un buen diseño deberá alinear los objetivos del negocio con los requerimientos técnicos. La visibilidad obtenida y levantada permite conocer que debe ser cambiado, eliminado, adicionado a la red existente para proveer mejor servicio. Inicia ya la validación a alto nivel de opciones de configuración (por ejemplo elección de protocolos de red), el detalle de documentación a este nivel es muy preciso.

En lo que respecta a documentos entregables de esta fase se tiene:

- **Documento de bajo nivel (LLD)**
- **Plan de Migración**
- **Pruebas de verificación del diseño**

Fase de Implementación

En esta fase se lleva a cabo la instalación delos equipos así como su configuración. En términos de proyecto el plan del proyecto debe ser cumplido, previo a proceder con la implantación debe ser acordado y aprobado por los miembros del equipo. El nivel de documentación obtenido debe proveer un detalle de cada paso a ser ejecutado así como el tiempo de ejecución pero fundamentalmente debe proveer un plan contingente y su respectivo rollback en caso de falla total. El objetivo principal que debe ser cumplido es el implementar los nuevos equipos sin comprometer la disponibilidad de la red y en caso de comprometerla debe definirse ventanas de mantenimiento. Es fundamental para cumplimiento de este objetivo el poder ejecutar un prototipo o piloto en un ambiente paralelo (de existir un ambiente de pre producción) o un segmento pequeño de producción (por ejemplo implementar en un área determinada) y/o de no disponer la posibilidad de ejecutarlo puede definirse mediante un prototipo ejecutado con herramientas existentes para el efecto que permiten simular un entorno real.

En lo que respecta a documentos entregables de esta fase se tiene:

- **Plan de implementación de red**

Fase Operativa

En esta fase se realiza tareas de monitoreo y administración de la red. Suele identificarse aquí posibles problemas de performance, temas que deben ser identificados, documentados y corregidos. Suele esta fase ser el paso final para cierre del diseño realizado. El objetivo principal

a cumplirse es el mantener un estado de salud óptimo de la red fin de brindar un mejor servicio, a su vez reducir las interrupciones y proveer mayor disponibilidad, fiabilidad y seguridad. A su vez debe ayudar a reducir costos y proveer acciones preventivas y correctivas inmediatas en lo posible que las mismas no presenten percepción del usuario final. Esta fase requiere de la implementación de herramientas de monitoreo de red, pueden ser las mismas que se usaron en la fase de Planeación. En lo que respecta a documentos entregables de esta fase se tiene:

- **Re creación de problemas**

Fase de Optimización

En esta fase se ejecutan acciones pro activas que resuelvan cuestiones identificadas en la fase de Operación, de presentarse demasiados problemas podría requerir una modificación del diseño realizado e incluso iniciar las fases anteriores. El objetivo principal es mejorar el desempeño de la red sin interrumpir la operación y adaptándose a las necesidades del día a día.

En lo que respecta a documentos entregables de esta fase se tiene:

- **Pruebas de aceptación del software**

2.4.4 Metodología de red bajo PPDIOO

Si bien el ciclo de vida PPDIOO establece 6 fases, la metodología de red bajo PPDIOO consiste de 3 pasos, mismos que forman parte de las tres primeras fases del ciclo de vida, siendo las siguientes:

1. **Identificar los requerimientos del cliente (Fase Preparación)**
2. **Caracterizar la red existente (Fase Planeación)**
3. **Diseño de la topología de red y solución (Fase de Diseño)**

Al culminar la fase de diseño se considera la construcción de un prototipo o piloto a fin de corroborar el diseño propuesto y solventar posibles problemas que se presenten.

Identificar los requerimientos del cliente

En términos generales se identifican los requisitos iniciales por parte de quienes toman decisiones, claro las mismas deben obligatoriamente basarse en objetivos de negocio. Estos requerimientos deben ser validados con usuarios finales, personal técnico, administradores, altos ejecutivos. De estas reuniones se debe determinar los objetivos y restricciones organizacionales y técnicos. Debe además definirse el alcance.

Los requerimientos iniciales de diseño son obtenidos por medio de documentos denominados RFI (Request for Information) o RFP (Request for Proposal) cuyo fin es solicitar información a proveedores acerca de un tema que se pretende solventar para un proyecto específico.

Recopilación de requisitos de red

El proceso de recopilación de requisitos se puede dividir en cinco pasos. Durante estos pasos (en lenguaje de proyectos denominado **hitos)**, el diseñador analiza el proyecto con el personal del cliente para determinar y reunir los datos necesarios, incluyendo la documentación apropiada, siendo los pasos:

1. *"Identificar las aplicaciones de red y servicios de red planificados*
2. *Determinar los objetivos de la organización*
3. *Determinar las posibles limitaciones de la organización*
4. *Determinar los objetivos técnicos*

5. *Determinar las limitaciones técnicas que deben ser tomados en cuenta",*

(Sholomon & Kunath, 2011).

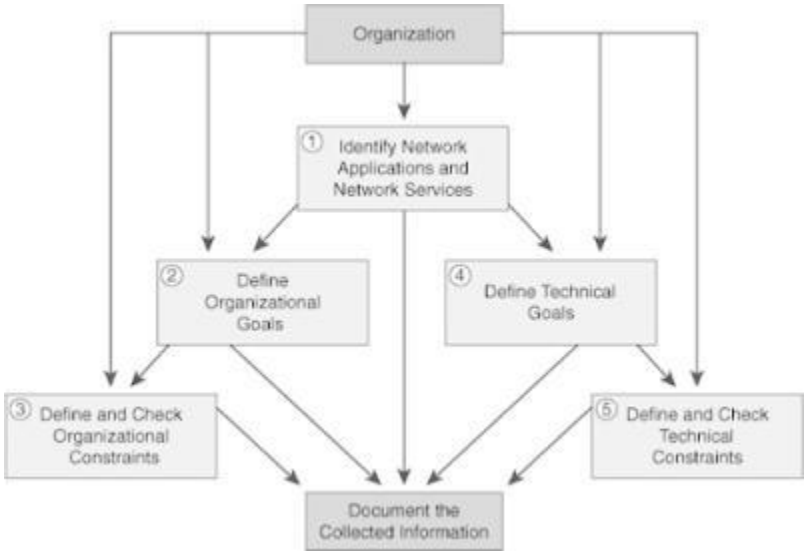

Figura 12. Identificar requisitos de diseño
Fuente: (Sholomon & Kunath, 2011)

Caracterizar la red existente

En términos generales se analiza el estado de salud de los componentes de la red con fines de determinar requerimientos de hardware o software. Su fin es modernizar y re estructurar la red. Para la ejecución de esta actividad se sirve de herramientas de recolección de datos que permiten evaluar y analizar la red.

Diseño de la topología de red y solución

Una vez que la red ha sido examinada y se han definido los componentes de la misma: es necesario crear un diseño de red. En primer lugar es indispensable el poder definir un diseño lógico para lo cual se recomienda el subdividir la red en módulos, mucho más si se trata de redes medianas o grandes.

Si bien esta tercera fase es la última de esta metodología dentro de la misma incluye la realización de un piloto o prototipo así como la puesta en producción. Es decir, esta fase incorpora las fases restantes del ciclo de vida.

2.5 Metodología PMI (PMBOK®)

"*El Project Management Institute (PMI) es una de las asociaciones profesionales de miembros más grandes del mundo; que cuenta con más de 600000 miembros con certificación vigente e individuos titulares de sus certificaciones en más de 190 países",* (PMI®, 2016). Se trata de una de las más importantes y atractivas certificaciones de proyectos a nivel mundial. Dentro de la misma consta el PMP® (Project Management Professional) que se figura como las más importante certificación del PMI, aunque existe un auge considerable en certificación PMI Agile Certified Practitioner (PMI-ACP) ® la misma que corresponde a metodología ágil; tema a su vez de gran interés actualmente en el mundo. El PMI se muestra como una organización sin fines de lucro que fomenta la profesión de la dirección de proyectos a través de estándares y certificaciones reconocidas mundialmente, a través de comunidades de colaboración, de un extenso programa de investigación y de oportunidades de desarrollo profesional. Se trata a su vez de un estándar reconocido internacionalmente el cual provee fundamentos para gestión de proyectos. Uno de sus productos más importantes: La Guía del PMBOK® provee una estructura coherente y un conjunto amplio de conceptos, lineamientos y términos compartidos por gestores de proyectos a nivel mundial. Presenta una diferencia con otro tipo de certificaciones, al requerirse justificaciones ante el PMI de experiencia en proyectos (por al menos 4500 horas) así como de un nivel de educación general (al menos estudios superiores) así como de educación en dirección de proyectos (al menos 35 horas), tal y como se ilustra en la figura 13.

Categoría	Educación General	Educación en Dirección de Proyectos	Experiencia en Dirección de Proyectos		Número de Preguntas
Uno	Título Universitario	35 horas de contacto	4.500 horas	Tres años	200
Dos	Certificado de Educación Media Superior	35 horas de contacto	7.500 horas	Cinco años	

Figura 13. Guía del PMBOK®
Fuente: (Mulcahi, 2013)

El PMBOK® como tal no se trata de una metodología de dirección de proyectos sino más bien de un marco de trabajo que contiene una colección de lo que se considera buenas prácticas para dirección de proyectos de cualquier tamaño, industria, tema fundamental al no estar delimitado a una determinada línea. La guía propuesta por el PMBOK® posee procesos, lineamientos, herramientas, técnicas y políticas para gerenciar proyectos.

Así, el orden para planear los procesos según el PMBOK®, se describe en la siguiente figura. *Estos procesos se pueden realizar en la secuencia presentada o de forma traslapada* (Garrido y Ramírez). No obstante, procesos tales como definir la integración y el alcance del proyecto, requieren ser definidos antes de continuar con los demás, pues ellos se constituyen en pilares para desarrollar los procesos restantes. Adicionalmente, la planeación de un proyecto puede estar estructurada de acuerdo con el orden como se presentan las diez áreas de conocimiento, mientras que para ejecutar los procesos, éstos pueden ser integrados e incluso, complementarse unos con otros. Se expone a continuación una gráfica de la interacción de los 5 procesos ilustrada en la figura 14.

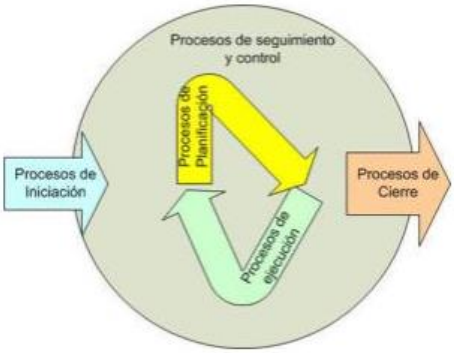

Figura 14. Cinco grupos de procesos del PMBOK®
Fuente: **https://formulaproyectosurbanospmipe.wordpress.com/2012/04/22/procesos-de-la-direccion-de-proyectos-para-un-proyecto-tema-n-3-26-03-2012-2da-parte-la-guia-del-PMBOK®-capitulo-3/**

2.5.1 Grupos de Procesos

2.5.1.1 Inicio

Los procesos de esta fase inician junto con la creación del proyecto o de una fase del mismo, su esencia se basa en identificar todos los interesados del proyecto, definir formalmente el alcance del mismo y brindar todo detalle que permita arrancar con el proyecto o fase como tal.

El grupo de Inicio permite definir y autorizar el proyecto o una fase del mismo.

2.5.1.2 Planificación

Los procesos de esta fase van direccionados en base al alcance que se ha definido al proyecto en base al esfuerzo, afinamiento de los objetivos planteados así como actividades requeridas para cumplirlas. Cabe mencionar que a medida que el proyecto avanza, se podrá tener mayores detalles del proyecto, lo cual puede generar la realización de re planificación, con lo cual esta fase está presente durante todo el desarrollo del proyecto.

El grupo de planificación permite definir, refinar los objetivos planteados y planificar todo lo requerido para lograr dichos objetivos.

2.5.1.3 Ejecución

Los procesos de esta fase están conformados en base a toda tarea que permita completar el trabajo definido en la planificación, este grupo requiere fundamentalmente el coordinar personas y recursos.

El grupo de Ejecución está compuesto por todo proceso que permite completar todo lo definido en la planificación.

2.5.1.4 Seguimiento y control

Los procesos de esta fase poseen relación directa con la ejecución en cuanto brinda la posibilidad de medir y observar cómo se van realizando los procesos de ejecución. A su vez brinda detalles para medir el rendimiento general del proyecto y brinda aporte para tener un mejor control de los posibles cambios y/o de acciones preventivas que permitan mitigarlos con anticipación.

El grupo de seguimiento y control permite medir, supervisar y regular el progreso del proyecto y/o identificar áreas en las que se requieran cambios.

2.5.1.5 Cierre

Los procesos de esta fase permiten el finalizar formalmente toda actividad de un proyecto o de una determinada fase así como la entrega del producto final.

El grupo de cierre formaliza la aceptación del producto final a su vez formaliza la aceptación de una fase y/o del proyecto.

Una vez validados los cinco grupos de procesos que interactúan en un proyecto es fundamental brindar un detalle gráfico de la interacción de los mismos dentro del rango de tiempo de un proyecto, el cual se ilustra en la figura 15.

Figura 15. Interacción de los grupos de procesos en un proyecto
Fuente: https://formulaproyectosurbanospmipe.wordpress.com/2012/04/25/3-la-interaccion-entre-los-procesos-de-la-direccion-de-proyectos-segun-la-guia-del-PMBOK®-26-03-2012-1ra-parte-la-guia-del-PMBOK®-capitulo-3/

"El PMBOK® representa el libro sagrado de la metodología de trabajo de PMI y describe diez ejes fundamentales interrelacionados que se enfocan en un claro objetivo: alcanzar unas metas preestablecidas sujetas a restricciones de costo, tiempo, calidad y alcance", (Garrido, Ramírez). Las diez áreas constan en la figura 16.

Figura 16. Diez áreas de conocimiento
Fuente: (Erazo, 2016), Elaboración propia

2.5.2 Áreas de conocimiento

2.5.2.1 Gestión de la Integración

Esta área de conocimiento interactúa con el resto de áreas existentes, como su nombre lo define es la integración de todos los procesos del resto de áreas de conocimiento (alcance, tiempo, costo, calidad, recursos, comunicaciones, riesgos, adquisiciones e interesados). Se trata de la única área de conocimiento que a su vez posee relación con todos los procesos definidos (inicio, planeación, ejecución, control y cierre). Es así que esta área es sumamente iterativa y sobre la cual el director debe recordar que toda área y proceso adicional llevan conexión. Por ejemplo, si se está realizando una estimación de costo, es necesario a su vez poder considerar el alcance, recursos disponibles, riesgos, y otros factores de otras áreas que puedan tener relación y/o verse afectados con dicha estimación. Bajo este mismo ejemplo y de tomarlo por separado es evidente el resultado no será el correcto.

Uno de los entregables más importantes de esta área es el acta de constitución del proyecto, el mismo que da inicio al proyecto como tal así como a otros procesos. Este a su vez genera el plan para la dirección del proyecto y además provee la dirección del cierre de una fase o del proyecto. Es fundamental que dentro del acta de constitución del proyecto conste la descripción del proyecto, responsable/ejecutor, justificación del requerimiento, recursos, interesados, alcance, supuestos, restricciones, mediciones, riesgos y patrocinadores. A su vez es importante el definir análisis económicos como son: costo-beneficio, retorno de inversión.

En lo que respecta al plan de dirección es fundamental el determinar los planes de gestión para cada área de conocimiento que ha de requerirse así como el mantener una

línea base a fin de poder comparar el desempeño en un momento dado. Debe incluir todo parámetro que defina reuniones, aprobaciones, interacciones no solo del proyecto sino de otros posibles con los que se tenga impacto, de manera que el plan brinde un detalle realista y formal. Se considera que durante la ejecución del proyecto pueden y han de presentarse cambios, los cuales deben ser formalizados a fin de evitar posibles desvíos del proyecto, los mismos deben ser registrados mediante controles de cambio y al igual que en el acta de constitución deben ser aprobados formalmente por el patrocinador, y estar bajo conocimiento y aceptación del resto de interesados, considerando desde su socialización que este puede provocar impactos (línea base, documentos.

Finalmente y como fue mencionado en líneas anteriores, esta área involucra el cierre de una determinada fase o del proyecto, para lo cual ha de garantizarse que el resultado ha sido elaborado en base a los requisitos, a su vez se deberá contar con una formalización de cierre por parte de los interesados así como de un acta de aceptación. Es fundamental el contar con una encuesta de satisfacción así como el definir lecciones aprendidas y causa raíz de los problemas encontrados y estos documentarlos en una base de conocimientos.

2.5.2.2 Gestión del alcance

Esta área del conocimiento se basa en definir el alcance el proyecto de manera de que se pueda completar otras actividades de planificación como son: costos, tiempos, calidad, comunicaciones, recurso humano requerido. Esta área de conocimiento posee relación con los procesos de planificación y de monitoreo y control. Posee dos temas principales a ser validados como son: alcance y el EDT (estructura de desglose del trabajo). En lo que respecta al alcance se refiere al trabajo que se requiere realizar para

entregar un producto, servicio o resultado, bajo características y funciones especificadas. Dentro del proyecto el alcance se orienta a todo entregable y actividad a ser realizada y que cumple con las especificaciones acordadas con los interesados. Es fundamental en esta fase se determine adicionalmente los supuestos y restricciones. Para una correcta validación del alcance y del EDT es fundamental el identificar correctamente los requerimientos. En cuanto se refiere al EDT se refiere a una descomposición jerárquica del trabajo en orientación de los entregables. Cada nivel que desciende del EDT ha de representar un nivel más detallado del trabajo del proyecto. A continuación un ejemplo de EDT, en donde comúnmente se tiene como el primer nivel del EDT al nombre del proyecto, a continuación el ciclo de vida del mismo; mientras que los niveles posteriores desglosa tareas más pequeñas hasta que se permita alcanzar un nivel apropiado. Se debe considerar que cada nivel lleva relación con entregables más no con actividades, se ilustra un ejemplo en la figura 17.

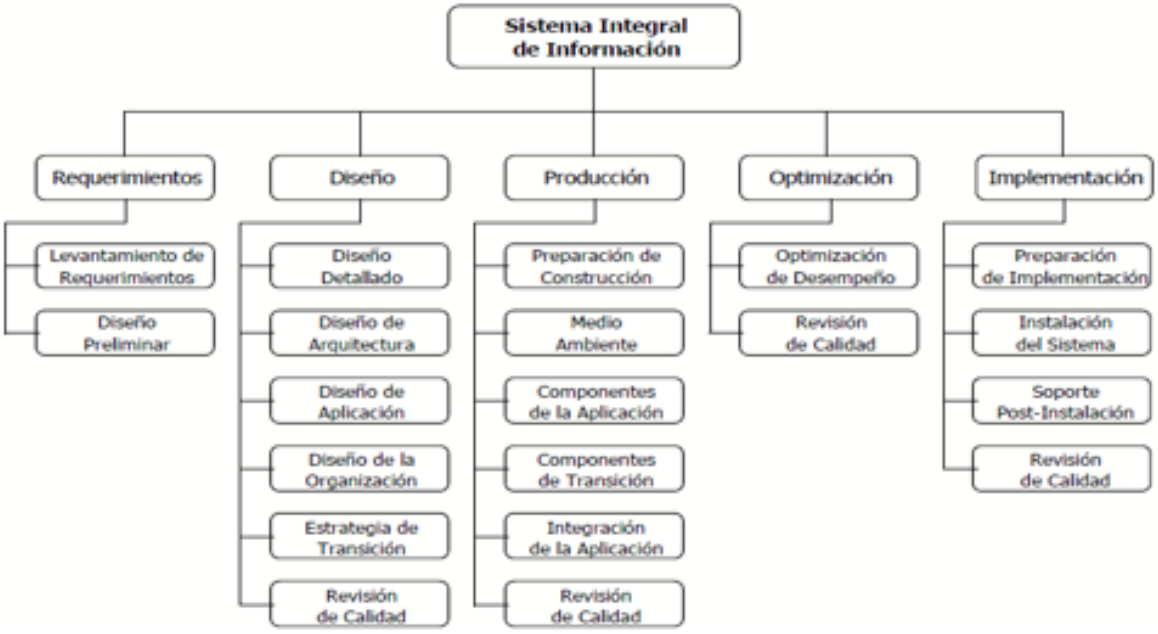

Figura 17. Ejemplo de EDT
Fuente: (Mulcahi, 2013)

2.5.2.3 Gestión del tiempo

Esta área de conocimiento se enfoca en la planificación del tiempo del proyecto. Al igual que otras áreas de conocimiento inicia con el proceso de planificación que brinda como resultado el plan de administración del cronograma, para luego relacionarse con el proceso de seguimiento y control al validarse la verificación de cumplimiento de actividades bajo el cronograma establecido. Centra adicionalmente su enfoque en estimar las duraciones de tiempo para actividades del proyecto, formar un cronograma y por supuesto el validar que el progreso y conclusión de las mismas permitan cerrar hitos, siendo este tema clave dentro de esta área.

2.5.2.4 Gestión del costo

Esta área de conocimiento se enfoca en la planificación del costo del proyecto. Al igual que en el área de gestión del tiempo inicia con el proceso de planificación que brinda como resultado el plan de administración del costo, para luego relacionarse con el proceso de seguimiento y control al validarse la verificación del costo actual versus el costo planeado. Centra adicionalmente su enfoque en estimar los costos para actividades del proyecto, determinar un presupuesto así como realizar mediciones que permitan mantener un control de costos permanente así como el poder establecer mecanismos que permitan lograra un mismo objetivo con el uso del menor valor del establecido. Mantiene enfoque con retorno de inversión.

2.5.2.5 Gestión de la calidad

Esta área de conocimiento se enfoca en la planificación de la calidad del proyecto. Al igual que otras áreas, inicia con el proceso de planificación a fin de obtener el plan de administración de la calidad, a continuación interactúa con el proceso de ejecución

brindando enfoque a definir y validar la calidad, esto a su vez conlleva el interactuar con el proceso de seguimiento y control a fin de llevar un control de calidad sobre los entregables del proyecto. Se centra adicionalmente en definir y chuquear procesos que afectan a todo el proyecto y en esencia en realizar validaciones de calidad a los entregables resultantes. Cabe mencionar que el proceso de calidad que establece la Guía de PMBOK® está alineado con la guía de administración de calidad de ISO (International Organization of Standardization).

2.5.2.6 Gestión de los recursos humanos

Esta área de conocimiento se enfoca en la planificación del recurso humano del proyecto. Al igual que otras áreas, inicia con el proceso de planificación a fin de elaborar el plan de administración del recurso humano para a continuación interactuar con el proceso de ejecución en donde se centra en formar el equipo del proyecto y direccionarlos a brindar soporte de la consecución de objetivos. Permite así identificar y establecer el apoyo a recibirse por parte del equipo durante la ejecución del proyecto. Esta área detalla además como recompensar, motivar y direccionar al equipo.

2.5.2.7 Gestión de las comunicaciones

Esta área de conocimiento se enfoca en la planificación de las comunicaciones dentro del proyecto. Al igual que otras áreas, inicia con la fase de planificación en donde se establece el plan de administración de comunicaciones del proyecto, a continuación interactúa con el proceso de ejecución en donde se lleva a cabo lo expuesto en la plan antes definido, e interactuar con el proceso de seguimiento y control realizando validaciones cualitativas de cómo se llevan a cabo las comunicaciones entre todos los involucrados.

2.5.2.8 Gestión de los riesgos

Esta área de conocimiento se enfoca en la administración de riesgos del proyecto, interactúa con la fase de planificación en donde se establecen y definen los riesgos y posee relación con el proceso de seguimiento y control en donde se brinda seguimiento a dichos riesgos.

2.5.2.9 Gestión de las adquisiciones

Esta área de conocimiento brinda su enfoque en la gestión de adquisiciones. Posee relación con el proceso de planificación en donde se forma el plan de administración de las adquisiciones que a su vez posee relación con el proceso de ejecución al ejecutar adquisiciones basado en el plan establecido. A su vez posee interacción con el proceso de seguimiento y control al realizar validaciones de términos contra actuales y a su vez con el proceso de cierre al validar y asegurar que todo contrato sea formalmente cerrado junto con el proyecto.

2.5.2.10 Gestión de los interesados

Esta área se enfoca en la administración de los interesados del proyecto, ante lo cual posee interacción con casi todo proceso. Su primera interacción se tiene con el proceso de inicio en donde se identifica los interesados de proyecto, a continuación interactuar con el proceso de planificación en donde se procede a definir el plan de administración de los interesados del proyecto, en lo que respecta al proceso de ejecución pone en marcha lo expuesto en el plan y lo que respecta al proceso de seguimiento y control se enfoca en validar que las actividades expuestas posean relación con los interesados intervinientes.

Así tenemos que se reconoce 5 grupos de procesos básicos y 10 áreas de conocimiento que son comunes a casi todos los proyectos, además de existir 47 procesos, que se despliegan a continuación, figura 18:

Figura 18. Procesos del PMBOK®
Fuente: (Mulcahi, 2013)

El comprender los procesos, área de conocimiento, procesos ayudará de sobre manera a la dirección y ejecución de proyectos. Más como ha sido expuesto esto solo brinda un marco de referencia y acercamiento a aspectos fundamentales a ser considerados por el autor.

Un aspecto adicional a ser considerado es la organización de la empresa en cuanto a proyectos se refiere. Dentro de la Guía del PMBOK® se especifica a la PMO (oficina de Dirección de proyectos) como el área en donde se centraliza y estandariza la dirección de proyectos. Usualmente una PMO brinda políticas, metodologías y plantillas para dirección de proyectos en una organización; bajo dicho lineamiento se la conoce como una **PMO de apoyo,** en otras ocasiones actúan como entes de control en cuyo caso es reconocido como una **PMO de control** mientras que si dicha área es la encargada de la dirección de los proyectos de la empresa se la conoce como una PMO de dirección. El rol que tenga la PMO depende del giro de negocio de cada organización más cualquiera de ellas integrará los datos e información de los proyectos estratégicos de la institución.

Según lo expone PMBOK® en su quinta edición, la PMO efectúa las siguientes directrices:

- *"Gestionar las interdependencias entre los proyectos, programas y portafolios*
- *Integrar la información de todos los proyectos para evaluar si la organización está cumpliendo con sus objetivos estratégicos*
- *Ayudar a proporcionar recursos",* (Mulcahi, 2013).

Es fundamental a su vez el mencionar que dentro del PMBOK® se conoce como un **programa** a un conjunto de proyectos que poseen relación. Se establece que un proyecto puede o no formar parte de un programa más un programa siempre constará de proyectos.

Existe además **portafolios** que son conjuntos de programas o proyectos que se priorizan con fin de lograr objetivos estratégicos.

De esta forma se ha brindado una introducción a conceptos de existentes en la Guía del PMBOK® así como una validación de los procesos que confirman parte del ciclo de vida, las áreas de conocimiento, los procesos así como una visión general del rol de la PMO en una organización y finalmente a relación existente entre proyectos, programas, y portafolios.

2.6 Metodología SCRUM

2.6.1 Breve introducción a AGILE

La metodología ágil (AGILE, del inglés) se forma adicionalmente de los siguientes objetivos:

Adaptativo

Guiado por objetivos

Iterativo

"Lean"

Emergente en el alcance

El termino anglosajón "Lean" hace referencia a realizar un trabajo sin pérdida de tiempo ni sobrantes, es decir bajo ofrecer un rendimiento superior, alta eficiencia y eficacia que permita trabajo sin errores, aumento de calidad, optimización de productividad y satisfacción del cliente.

Es fundamental realizar una referencia a lo expuesto por acerca del manifiesto ágil; de donde cabe puntualizar que "*cualquier metodología basada sobre manifiesto ágil brinda menor valor a temas que para métodos tradicionales son fundamentales: como lo*

es seguir un plan, cumplir procesos y efectuar documentación a fin de generar entregables, cabe mencionar que esto no indica que no lo ejecute", (Beck y otros, 2001).

Figura 19. Manifiesto ágil.
Fuente: http://agilemanifesto.org/iso/es/

En el año 2001, los proponentes de estas metodologías de peso liviano se encontraron para conformar la "Alianza Ágil" y publicaron un manifiesto en común y establecieron 12 principios. Las prácticas que se adhieren a este manifiestos y a sus principios se denominan Metodología Ágil. Los principios a continuación expuestos fueron desarrollados en dicho manifiesto.

1. Satisfacer al cliente a través de entregas tempranas y continuas.

2. Dar la bienvenida a requerimientos cambiantes (CRs), incluso si es tarde respecto al desarrollo.
3. Entregar frecuentemente software en funcionamiento.
4. El negocio y los desarrolladores deben trabajar juntos a diario.
5. Construir proyectos entorno a individuos motivados.
6. Conversar cara a cara es el método de colaboración más eficiente y eficaz.
7. El software en funcionamiento; es la principal medida de progreso
8. Los procesos ágiles promueven el desarrollo sostenible.
9. La atención continua, la excelencia técnica, y el buen diseño mejoran la agilidad.
10. Maximizar el trabajo no realizado.
11. Los mejores resultados surgen de equipos auto-organizados.
12. Con intervalos regulares, el equipo reflexiona y ajusta su comportamiento respectivamente

Scrum forma parte de metodologías ágiles; la cual ha obtenido un amplio despliegue de uso en los últimos años especialmente para ejecución de proyectos de desarrollo de software y por supuesto en otras áreas e industrias. La razón principal de su despliegue radica que frente a metodologías tradicionales brinda solución más pronta a temas que han sido expuestos por los intervinientes (stakeholders) y que han causado generalmente problemas en la ejecución de proyectos; entre los cuales se tiene: entrega no se cumple al tiempo ofrecido, el resultado final cuesta mucho más de lo presupuestado, existe demasiada documentación, se presentan muchos

cambios, metodología presenta fallas, el resultado obtenido no se ajusta a lo solicitado, usuario no sabe lo que quiere. Es decir contempla varios puntos de vista de los diferentes intervinientes que usualmente forman parte del proyecto a lo cual se suma que tradicionalmente las metodologías conllevan mucho tiempo en fases de análisis, diseño y lo propio en etapas de pruebas, despliegue, de donde al llegar al 90% de ejecución del proyecto el valor aportado es casi nulo. Es así que una metodología AGIL provee un desarrollo incremental puesto que aporta entregas periódicas, tangibles al usuario final, aportando así valor desde su primera iteración. Incluso dentro de la metodología ágil; el valor aportado al inicio del proyecto puede ser mayor al presentado al final, más puede incluso añadir mayor valor en cada iteración (al existir entregables permanentes) y permitir así brindar mayor valor que el esperado al final de dichas iteraciones. Se busca así que las entregas brindadas pasen de ser predictivas (modelo en cascada) a ser entregas agiles, brindando un mejor feedback al usuario final, tal y como se ilustra en la figura 20.

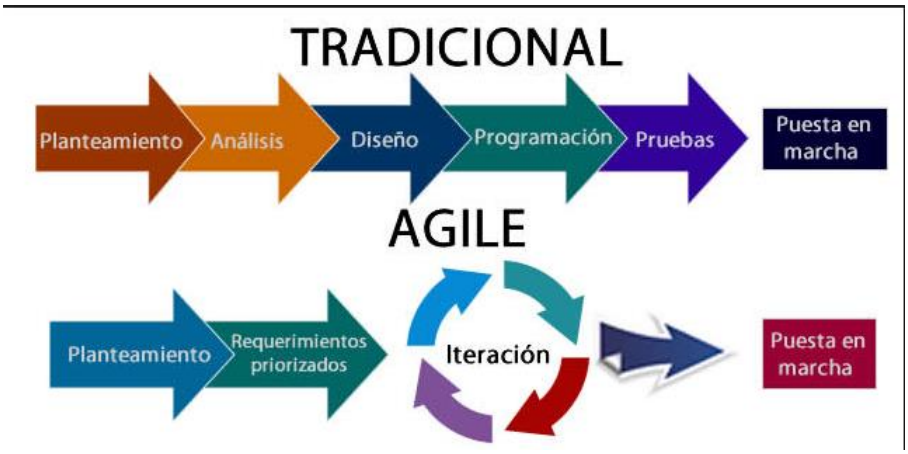

Figura 20. Evolución de una entrega predictiva a una adaptativa
Fuente:
https://www.google.com.ec/search?q=scrum+vs+metodologias+tradicionales&biw=1366&bih=622&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiO4sq5m-rQAhXHSSYKHV9dAx0Q_AUIBigB&dpr=1#imgrc=96iDki72BI5fQM%3A

Entrega predictiva (modelo tradicional)

- Amplio esfuerzo en etapas de Análisis, Diseño, Pruebas y Despliegue
- Construir el producto planificado en el tiempo y costos previstos

En la figura 21 se puede evidenciar que al usar una entrega predictiva, debe esperarse un tiempo y costo establecido para obtener un producto.

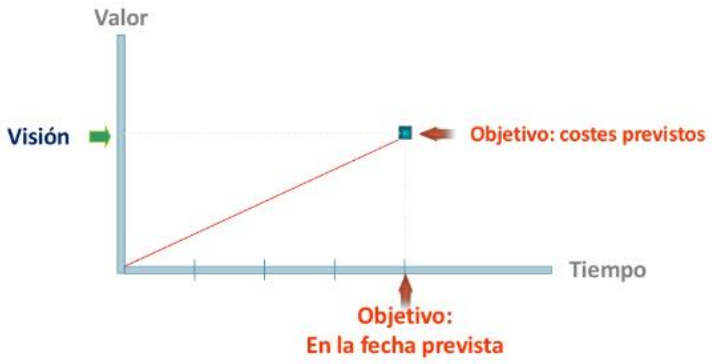

Figura 21. Entrega predictiva.
Fuente: http://es.slideshare.net/JuanPalacio2/gestin-agil-y-entrega-de-valor

Una vez obtenido el producto a ser probado puede ser validado con el cliente. En adelante y de haber cumplido lo esperado podría ser entregado a tiempo (caso optimista) brindando un valor al cliente, representado para el caso en el cuadrado de color azul de la figura 22.

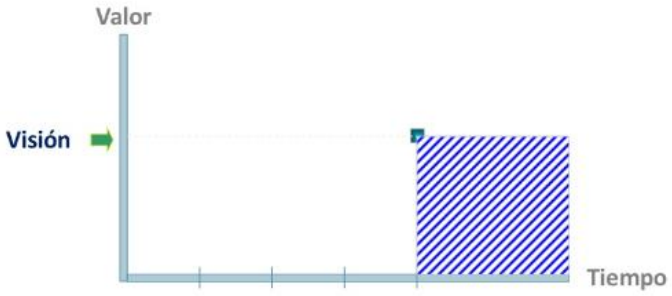

Figura 22. Entrega predictiva 2.
Fuente: http://es.slideshare.net/JuanPalacio2/gestin-agil-y-entrega-de-valor

Entrega adaptativa (modelo ágil)

- Presenta un desarrollo incremental, a su vez aporta una entrega de valor incremental ante el cliente, se ilustra en la figura 23
- Permite anticipar nuevas posibles necesidades las cuales pueden ser incorporadas sin causar afectación en el tiempo

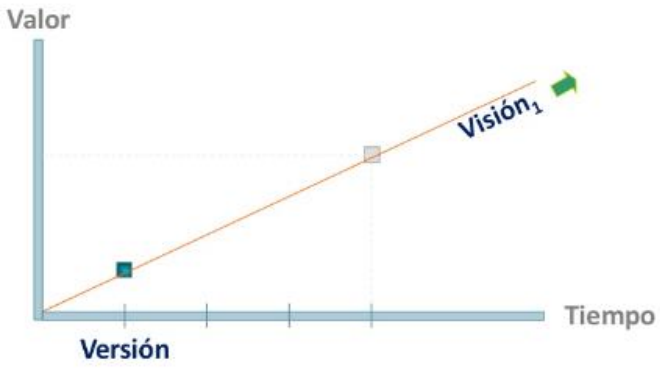

Figura 23. Entrega adaptativa.
Fuente: http://es.slideshare.net/JuanPalacio2/gestin-agil-y-entrega-de-valor

En un momento dado (para el caso de la figura 23), permite al cliente visualizar el avance obtenido, generando valor y permitiendo confirmar el cumplimiento de la visión general esperada, a su vez podría permitir incrementar el valor del resultado esperado (como se muestra en figura 24).

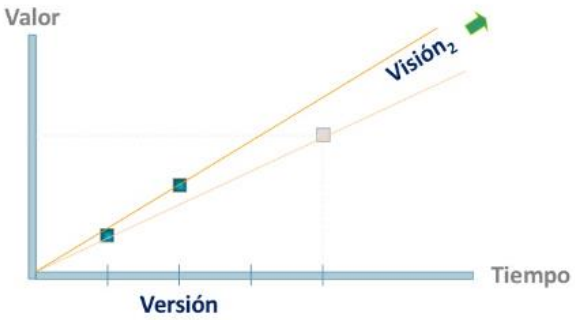

Figura 24. Entrega adaptativa 2.
Fuente: http://es.slideshare.net/JuanPalacio2/gestin-agil-y-entrega-de-valor

Es así que permite que el resultado final pose mayor valor de entrega ante el cliente, tal y como se muestra en la figura 25 mediante el área marcada en color naranja y azul.

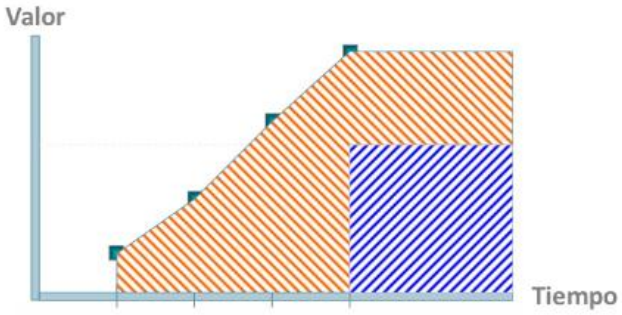

Figura 25. Entrega adaptativa 3.
Fuente: http://es.slideshare.net/JuanPalacio2/gestin-agil-y-entrega-de-valor

Diferencias entre entrega predictiva y adaptativa

Bajo un proceso de entregas predictivas, la metodología se rige bajo un plan mientras que en un proceso de entregas de tipo adaptativo, se guía por la calidad.

Realizando una comparación en lo que respecta al desarrollo del ciclo de vida se podría decir que la metodología ágil posee varias versiones de las distintas etapas presentando en cada una de ellas un producto listo para ser usado. Difiere totalmente de una metodología tradicional que la misma no es útil hasta culminar con la misma.

2.6.2 Generalidades de Scrum

En cuanto se refiere a Scrum se trata de una metodología muy simple pero que requiere de trabajo muy duro ya que no se basa en seguir un plan (como en metodologías tradicionales) sino en una adaptación continua resultante de las circunstancias de la evolución del proyecto. Se basa en los principios antes definidos de donde el recurso humano es mucho más importante que los procesos.

2.6.2.1 Visión

Es esencial como primer punto de un proyecto en Scrum, el detallar la meta del negocio y es liderada y generada por el **Product Owner** quien es la persona que comprende a fondo las necesidades del cliente, es capaz de comunicar y crear la visión del producto, además de ser quien toma decisiones dentro de un proyecto Scrum.

2.6.2.2 Componentes básicos de Scrum

Dentro de los componentes esenciales de Scrum se tiene: Artefactos, Prácticas y Roles.

2.6.2.2.1 Artefactos

Pila de Producto (Product Backlog)

Es una lista de características priorizada que contiene descripciones cortas de todas las funcionalidades deseadas para un producto. Es usual que el equipo de Scrum y el product owner empiecen por escribir todo lo que venga a sus mentes acerca de ítems que deben constar en el mismo; siendo por lo general el primer sprint que se forma. Esto evidencia que el **product backlog** es cambiante en el tiempo y detalla el entendimiento total del producto. Suele a su vez llevar un formato que incluye los siguientes parámetros: nombre, importancia, estimación inicial, como probarlo, notas. En la figura 26 se muestra un ejemplo de pila de producto.

Pila de Producto (ejemplo)					
ID	Nombre	Imp.	Est.	Como probarlo	Notas
1	Depósito	30	5	Entrar, abrir página de depósito, depositar 10€, ir a página de balance y comprobar que se ha incrementado en 10€	Necesita un diagrama UML. No preocuparse por encriptación aun
2	Ver tu historial de transacciones	10	8	Entrar, ver transacciones. Realizar un depósito de 10€. Ir a transacciones y comprobar que se ha actualizado con el nuevo depósito	Utilizar paginación para no hacer consultas muy grandes a la BB DD. Diseño similar a la página de usuario.

Figura 26. Ejemplo de un product backlog
Fuente (Silvano, 2015)

Sprint Backlog

Contiene historias del usuario seleccionadas por el equipo, mismas que se encuentran totalmente estimadas y divididas en tareas. El seguimiento al progreso de los sprints se ejecuta mediante herramientas de software o mediante tableros muy sencillos de seguimiento, mismos que pueden ser gestionados por cualquier miembro del equipo, no solamente por el Product Owner o Scrum Master. Las historias de usuario proveen una descripción de cómo interactúa un usuario con el producto; suelen ser definidas respecto al formato:

Como usuario <tipo de usuario>

Quiero <define característica>

Co el fin de <detalla beneficio>

Ejemplo:

Como administrador de la Intranet, quiero estar en capacidad de crear encuestas dentro de la aplicación con el fin de poder obtener resultados ante diferentes aspectos que sean requeridos por la institución

Las historias de usuario suelen dividirse en tareas, y respecto al seguimiento suele definir: tareas a realizar y/o en curso, tareas en progreso, tareas por validar/probar y tareas ejecutadas. En la figura 27 se expone un formato y ejemplo de historias de usuario.

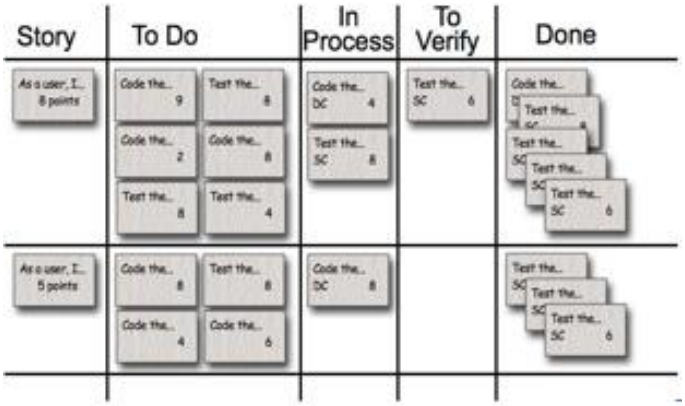

Figura 27. Ejemplo de historia de usuario
Fuente (Silvano, 2015)

Gráficos Burn down

Es usado para mostrar el progreso de las tareas completadas en un Sprint. Permite visualizar si van o no a poder conseguirse los objetivos de un determinado Sprint. Se trata de un gráfico que valida el número de horas de trabajo restante (puntos de historia) en relación a un periodo de tiempo. Es fundamental en un proyecto Scrum este diagrama sea actualizado diariamente y que pueda ser visto por cualquier persona que lo requiera, a continuación un ejemplo representado en la figura 28.

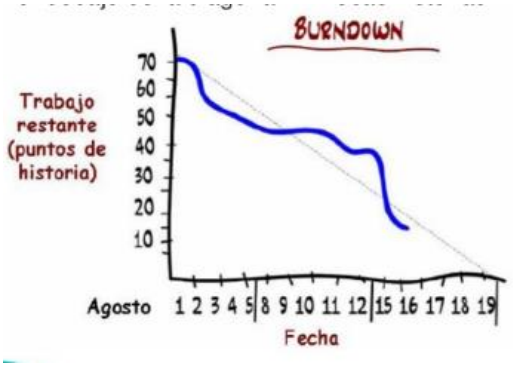

Figura 28. Gráfico Burn Down
Fuente (Silvano, 2015)

2.6.2.2.2 Prácticas

Sprint

Se refiere a iteraciones del equipo Scrum que suelen llevarse en sesiones de 30 días en las cuales se planea una meta que se expresa en términos de negocio, suele caracterizarse por no ser reuniones muy largas, además suele tratar en tema en específico de la pila de Sprint y por ende de esta reunión se detallan historias de usuario para dichas pilas. Cuando existe ya entregables; se suele en estas reuniones efectuar una demostración a los participantes. A continuación se detalla el ciclo de sprint mediante ilustración en la figura 29.

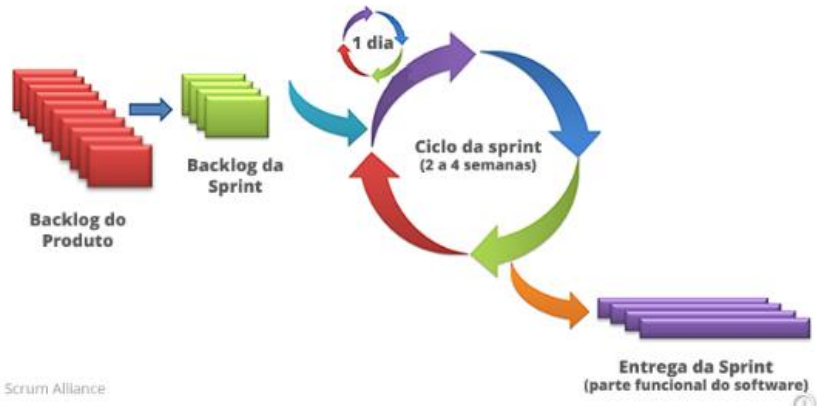

Figura 29. Ciclo de sprint
Fuente: http://www.synergia.dcc.ufmg.br/wp-content/uploads/2014/03/scrum-ciclo.png

En un Sprint pueden presentarse cambios, para esto puede cambiarse una historia, misma que puede ser resultante de un cambio de alcance, cambio de prioridad y/o necesidad de subdividirla. En cuanto a desechar una historia solo es factibles si:

- La tecnología seleccionada no funciona
- Las circunstancias del negocio han cambiado
- E equipo ha tenido muchas interferencias

Esta actividad solo puede ser ejecutada por el Scrum Master.

Planificación del sprint

Se trata de reuniones en donde se suele definir el product backlog, Sprint backlog, y donde se planifica toda actividad que lleva compromiso con el alcance definido. En estas reuniones deben considerarse todos los riesgos potenciales y problemas que se presentan, se trata de reuniones que constan con participación del Scrum Master, Miembros del equipo Scrum y el Product Owner. En cuanto a periodicidad esta reunión se lleva a cabo cada inicio de un sprint y debe ser ejecutada en 2 a 3horas.

Scrum diario

Adicionalmente se cuenta con reuniones diarias usualmente llevadas a cabo antes del final de la jornada de trabajo con una duración no mayor a quince minutos cuyo fin es comentar los avances de progreso efectuados, actividades a ser ejecutadas al día siguiente y adicionalmente detalla cualquier problema que no permita la normal continuidad al día siguiente y/o que se haya presentado en el

día. Su objetivo es que cada miembro del equipo contribuya en encontrar soluciones; es así que no se trata de una reunión diaria de actualización de estado, seguimiento sino más bien de una reunión donde se resuelve problemas.

Revisión del sprint

El objetivo de la revisión de un sprint es el interactuar con todos los equipos, direccionar a que las actividades planificadas sean cerradas según su planificación. La revisión no se ejecuta en términos técnicos sino a nivel de negocio

Retrospectiva de Sprint

Se trata de un foro en el cual se comparte lo positivo y negativo que se tiene en las actividades. Adicionalmente es poder validar acciones de seguimiento para mejorarlas.

2.7 Herramientas y técnicas útiles para entregables de las distintas metodologías

2.7.1 Modelo de Proceso ETVX

El modelo ETVX (de las siglas en ingles Entry-Task-Validation, Exit [Entradas, Actividades/Tareas-Validaciones-Salida]) ordena los procesos a ser realizados en base al seguimiento del contexto:

1. Insumos o factores desencadenantes
2. Tareas/actividades (usualmente llamadas procedimientos)
3. Controles de validación a ser realizados
4. Posibles limitaciones a generarse
5. Salida (entregable, puede ser usado como insumo de otra fase posterior)

A continuación, en la figura 30 se aporta una gráfica que detalla el modelo ETVX.

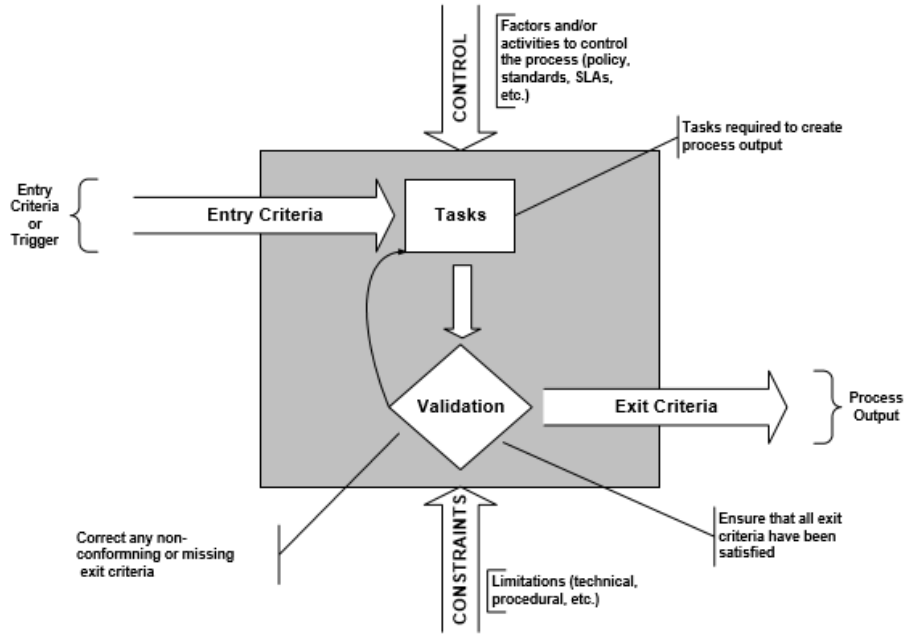

Figura 30 Modelo ETVX
Fuente: http://slideplayer.com/slide/9387919/

Se trata de un proceso de calidad que define las entradas correctas y lleva a cabo toda acción requerida para producir productos que cumplan con las necesidades definidas y acordadas con el cliente incluyendo principalmente: aptitud para el uso, provee las salidas correctas, entregables generadas a tiempo y en el lugar correcto además de proveer satisfacción del cliente.

Criterios de ingreso (**Entry**): definen entradas/insumos a ser requeridos, mismos que usualmente suélense salidas de un procesos previo.

Definición de actividades (**Task**): son los componentes de acción de un proceso. Este paso asegura que el proceso no genere una salida sino hasta haber culminado con todo criterio de salida, mismo que debe ser cumplido a cabalidad.

Validación de definiciones (**Validation**): se trata de un punto de control que se genera una vez que el proceso ha sido completado y su propósito es asegurar que toda actividad haya generado salidas que cumplan con las especificaciones definidas. De existir falla en algún punto de control deberá ejecutarse nuevamente el proceso.

Criterios de Salida (**Exit**): define las salidas requeridas que llevan inmersas la calidad en base a las necesidades del cliente. Estas necesidades suelen ir derivadas a su vez respecto a un nuevo proceso de entrada.

2.7.2. Técnicas de identificación de problemas y toma de decisión

Las herramientas a continuación citadas permiten brindar apoyo en la toma de decisiones así como en la detección de problemas pudiendo estos ser: de tipo rutinario o nuevo. A continuación los métodos más usados de forma general:

Foros

Considera reunir a un grupo de trabajo establecido en donde se realiza un debate abierto en base a un determinado tema, hecho o problema. Debe considerar la participación de todo involucrado de donde se busca obtener diferentes puntos de vista

Técnica de Grupo Nominal

Considera reunir a un grupo pro su objetivo no es la comunicación entre los mismos sino en presentar los diferentes problemas y brindar a cada miembro en presentar su idea ante el problema a todo el grupo misma que es evaluada por cada uno de ellos. La decisión final s ser tomada parte de la idea que obtenga la calificación más alta.

Lluvia de ideas

Permite consolidar diferentes ideas acerca de un tema, hecho o problema

Diagrama de Ishikawa

Debido a su estructura suelen denominarlo diagrama de espina de pescado, mismo que consiste en representar gráficamente un problema a analizar. Evidencia relaciones múltiples de causa efecto entre diferentes variables intervinientes. Suele basarse sobre ciertos parámetros como son: entorno, maquinaria, factor humano, materiales, métodos, medidas, tal y como se representa en la figura:

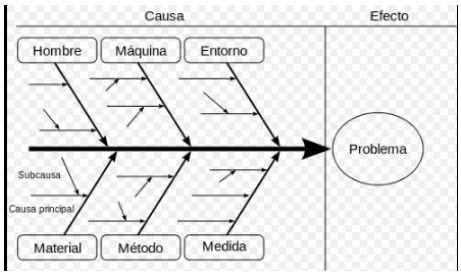

Figura 31 Diagrama de Ishikawa

Fuente: https://es.wikipedia.org/wiki/Diagrama_de_Ishikawa#/media/File:Diagrama-general-de-causa-efecto.svg

Principio de Pareto

Es utilizado como herramienta de gestión y control de calidad que permite brindar control al 20% de los defectos que puedan presentarse y que pueden afectar al 80% de los procesos. Al definir y establecerlos permiten identificar problemas relevantes que acarrean el mayor porcentaje de error.

CAPÍTULO III

METODOLOGÍA PROPUESTA

3.1 Introducción

El presente capítulo expone un estudio comparativo de las diferentes metodologías que fueron citadas por el autor, y que forman base esencial en la metodología a ser propuesta. Se procede a analizar los pros y contras que poseen cada una de las metodologías de manera que permita definir y establecer las entradas, tareas, actividades y salidas que formarán parte de la metodología propuesta. El objetivo del presente capítulo es el establecer una metodología que permita presentar una propuesta aplicable al manejo de proyectos de redes en una institución financiera cuyo objetivo principal es el establecer una gestión eficiente de red con altos parámetros de disponibilidad y seguridad definiendo para el caso entregables en fases que garanticen el obtener un buen diseño, implementación, operación y mantenimiento de la red y que a su vez permitan definir actividades para las diferentes fases del proyecto junto a su respectiva validación de calidad. A su vez definir actividades que permitan establecer lineamientos que aporten al monitoreo y mejora del desempeño de la red. Finalmente permita incorporar los entregables de las diferentes fases del proyecto hacia el cumplimiento de los objetivos del negocio, optimización de la red, exigencias de unidades internas de control así como entidades externas y entes regulatorios, permitiendo así cumplir con normativas vigentes.

3.2 Estudio comparativo metodologías de Proyectos

Metodologías de proyectos versus metodologías de redes

Es fundamental realizar una comparativa de las diferentes metodologías de proyectos de redes y proyectos en general que fueron citadas en el capítulo anterior con fines de poder

establecer todo lineamiento a ser considerado en la metodología propuesta por el autor. La base inicial a ser considerada es que el área de tecnología de la entidad financiera maneja un presupuesto anual considerable que a menudo no refleja un correcto retorno de inversión y cuyo costo suele ser mucho más elevado respecto al que inicialmente fue proyectado; adicional de denotarse la presencia de alcances muy distintos a los inicialmente fueron propuestos. Esta problemática justifica la necesidad de efectuar cambios en la administración de proyectos de tecnología.

En lo que respecta a las metodologías de red citadas en el capítulo anterior poseen como objetivo principal el apoyar al diseño de la red con fines de proveer una mayor disponibilidad de red, escalabilidad y agilidad para realizar cambios en la misma (de ser requeridos). Es así que se consideró PPDIOO que en términos muy generales provee un modelo de implementación para cualquier cambio en la red existente sea este pequeño o grande a su vez a Top Down que suele ser usada para proyectos de diseño de red; misma que basa su esencia en el modelo de referencia OSI y sus 7 capas. Top Down considera así un cuidado exhaustivo en el diseño de red manteniendo presente el cuidado ante los objetivos de seguridad y del negocio, centrándose adicionalmente en efectuar sus acciones desde la capa más alta de OSI para luego detallar capas inferiores de la misma. Sus fases plenamente identificadas definen los pasos a seguir que parten de la identificación de las necesidades del cliente y de los objetivos del negocio para luego poder identificar el diseño lógico a seguir mismo que se complementa con el diseño físico para finalmente realizar las pruebas, optimización y documentación del diseño de red. Mediante el desarrollo de las fases se brinda solución y seguimiento a las necesidades del negocio así como a todo detalle técnico; a su vez provee cierto grado de información propia del proyecto en términos de alcance, esfuerzo y costo; más no ocurre lo propio en términos de manejo de

riesgos, control de cronograma establecido, control de calidad, de comunicaciones con los integrantes del proyecto, adquisiciones realizadas mucho menos define lineamientos a ser adecuados en una empresa para el manejo y dirección del proyectos.

PPDIOO por su parte centra su objetivo principal en disminuir el costo de la administración total de red y brindar aumento en la disponibilidad de la misma, sus fases (constan las 3 primeras establecidas para el ciclo de vida PPDIOO) basan su esencia en la identificación de requerimientos del cliente, evaluación de la red existente para finalmente proveer el diseño de la topología de red y la solución a ser implementada. Presenta dentro de esta última fase una definición acerca de la implementación a ser ejecutada, lineamientos para el mantenimiento de la misma así como lineamientos para optimización y mejora continua siendo el diferenciador de esta metodología. En cuanto a criterios propios de proyectos y al igual que en el caso de Top Down no establece lineamientos respecto al manejo y dirección de proyectos, cabe mencionar si detalla entregables pero ninguno de ellos bajo esta perspectiva, es así que se evidencia la necesidad de acoplar estas metodologías con criterios de proyectos en general. Para el efecto se ha citado en el capítulo anterior las metodologías PMI y Scrum mismas que en cambio aportan en el complemento de definición de lineamientos para monitoreo y ejecución de proyectos durante el desarrollo de las fases definidas. Cabe acotar que no se menciona con lo expuesto que las metodologías Top Down y PPDIOO no posean fases estructuradas sino en potenciar las mismas mediante técnicas y habilidades que se han definido para dirección de proyectos, tampoco se pretende exponer que estas metodologías citadas (PMI, Scrum) sean la únicas opciones más si las citadas en el presente documento como posibles para dirección de proyectos en general.

Se considera en primera instancia el recoger lineamientos del ciclo de vida en cascada a fin de definir actividades secuenciales que permitan llevar un correcto control y documentación y a su vez poder definir actividades flexibles que puedan ser paralelizadas entre fases y que permitan dar prontas soluciones y apoyen en la identificación temprana de posibles riesgos o problemas, identificando plenamente tareas que pueden ser ejecutadas en paralelo con otras y tareas que deben seguir una secuencia definida. Se puntualiza la necesidad de contar con actividades de seguimiento y control durante cada una de las fases a ser definidas con fines de llevar un correcto control del proyecto y prevenir así posibles problemas. Un aspecto fundamental dentro de las metodologías de proyectos y en caso específico de PMI es la referencia existente acerca de la definición de una PMO (oficina de dirección de proyectos), misma que es esencial al hablar de manejo de proyectos dentro de una organización. Se recoge de Scrum su alta flexibilidad para incluir cambios durante el desarrollo sin perder de vista el objetivo central. Si bien existen múltiples diferencias entre PMI y Scrum ambas parten de la necesidad de definir desde su fase inicial el tamaño del proyecto, tema esencial para la definición de actividades de fases sub siguientes y para toma de decisión por parte del equipo ejecutar para seguir una u otra definición y/o acoplarlas (de aplicar). A su vez poseen similitud en su resultado final, es decir la entrega de un producto que cumpla las expectativas formuladas, su principal diferenciador viene marcado en factores del proceso propio de cada metodología: PMI centra su objetividad en el cumplimiento de un plan, en los grupos de procesos definidos y en el cumplimiento y documentación de los mismos, mientras que para Scrum su objetividad se centra en la calidad, visión prestando interés en las personas y en entrega continua de resultados. Mientras PMI se centra en un plan y en crear estimados para costos/calendario; Scrum se centra la visión y en creación de estimados de características. Este enfoque ha marcado una tendencia

en el uso y despliegue de metodologías agiles al proveer resultados incrementales y más oportunos frente a metodologías más tradicionales como PMI (valga acotar PMI ofrece ya lineamientos para metodología ágil, en el presente documento no citados). Se tiene así definido en términos muy generales que el uso de metodologías tradicionales trae consigo generalmente algunos problemas ya conocidos: entrega no oportuna, costo elevado frente a lo presupuestado, muy alto grado de documentación, demasiado tiempo usado en etapas tempranas así como de pruebas, generando un resultado/producto final obtenido ya no suple toda expectativa proyectada; tema que lo solventa Scrum en donde al existir un desarrollo incremental con entregas periódicas y al ser muy flexible permite obtener un producto final con características adicionales a la expectativa inicial proyectada.

3.3 Metodología Propuesta

En base a los lineamientos expuestos en el capítulo anterior y bajo la comprensión de las necesidades requeridas en la institución financiera así como del entorno en la que se desenvuelve; se han definido fases, actividades, entregables en base al modelo ETXV de manera que se simplifique la misma y determine los pasos a seguirse, sin pretender los mismos sean rigurosos sino de apoyo ante el ejecutor. El objetivo principal de la presente es acoplar una metodología personalizada basada en lineamientos ya existentes y definidos en las metodologías de redes Top Down y PPDIOO así como para PMI, Scrum y proveer un marco referencial que permita al ejecutor aplicarlos de manera que se brinde cumplimiento tanto a los objetivos técnicos como los del negocio. A su vez brinde una correcta documentación, monitoreo y mantenimiento continuo. Si bien el resultado está enfocado específicamente para el manejo de proyectos de redes se ha acoplado de tal forma que brinde solución manejo de proyectos de Infraestructura (redes/servidores/storage).

Previo a desplegar la metodología como tal y con fines de brindar realce al objetivo del presente trabajo; es importante evidenciar la situación actual que enfrenta en área de redes y comunicaciones dentro de la institución financiera que a su vez responde a un problema generalizado dentro del área de tecnología de las instituciones públicas como privadas, en donde el uso de una metodología de proyectos no es usualmente aplicado; generando graves problemas en el manejo de presupuestos, manejo de documentación, apoyo al negocio con retorno de inversión, entre otros.

Situación actual

La institución financiera en donde se ejecuta la investigación ha experimentado varios cambios en su estructura tecnológica debido a objetivos del negocio que la han requerido y ante una expansión notable que ha tenido en los últimos años. En lo que respecta a la infraestructura de redes y comunicaciones ha debido acoplarse a estos lineamientos realizando para el efecto varios cambios. Se ha denominado como "cambios" a pesar que cada uno de ellos ha correspondido a un proyecto ejecutado con su respectivo presupuesto y bajo un determinado alcance, ejecutor/responsable. Lastimosamente por temas culturales, jerarquía existente, entre otros; ninguno de ellos fue ejecutado en base a lineamientos de una metodología de proyectos, generando un primer problema que es no contar con una correcta documentación detallada de los mismos, tampoco con un control del presupuesto durante ejecución. Si bien el alcance requerido estaba definido este no consta como formalizado en documento alguno. Se evidencia a su vez existir graves problemas de documentación al no generarse formalizaciones de cambios en el diseño general de la red, oficialización de permisos firewall generados durante la ejecución de los cambios, lineamientos establecidos, etc. La poca documentación existente se basa en mínimas definiciones establecidas que en general brindan un detalle macro de la solución a

implementar, proveedores/ejecutores internos a cargo y presupuesto asignado. Cuando se ha obtenido mayor información ha sido cuando existe un proveedor de por medio asignado a dicho cambio; en donde se define ya un alcance, plazos, costos, responsabilidades, pre requisitos, más aún en estos casos el detalle no es muy específico pues responde a una propuesta económica ante un pedido.

Con implementación de auditorías internas y bajo exigencias de resultados de auditorías externas este nivel de documentación ha ido aumentado pero en ningún caso ha brindado detalle a nivel de una metodología de proyectos. Por otro lado cabe mencionar dicha institución no posee un área, oficina o departamento que brinde gerenciamiento interno de proyectos, por ende no han existido capacitaciones en referencia a manejar estos temas por parte de los colaboradores del área de tecnología en base a una metodología. Se evidencia eso si el existir por otras áreas procesos plenamente definidos para políticas, normas internas mismas que están correctamente documentadas y bajo disponibilidad de cualquier colaborador de la institución, para el efecto guardadas en un servidor de archivos local así como en un gestor documental (SharePoint).

La poca información existente de cambios, diagramas, diseños de red, e información relevante al área si consta en los dos repositorios antes mencionados. Se evidencia adicionalmente existir el uso de metodología MSF por medio del área de desarrollo de aplicaciones más la misma no evidencia la suficiente documentación a nivel de proyectos. Se ha definido crear documentación para cambios efectuados por el área de Infraestructura (redes, servidores, storage, BDD) más la documentación existente responde a la antes referida en donde se evidencia solo información a muy macro nivel.

Bajo esta perspectiva y con fines de brindar una solución que permita llevar y mantener un mejor control de todo cambio que involucre a la Infraestructura de red, se ha procedido a definir la metodología continuación citada.

Solución presentada (Metodología propuesta)

En base a las metodologías citadas, se ha establecido una metodología complementaria compuesta por 9 fases, una de ellas con actividades marcadas dentro de cada fase (monitoreo y control); a su vez 8 fases cuyo fin es el definir, establecer y ejecutar toda actividad que permita obtener el resultado / producto final esperado. Como ha sido mencionado el objetivo principal de esta metodología es presentar una solución acorde a las necesidades de la institución, con fines de brindar lineamientos que apoyen a los colaboradores de la misma en la ejecución de proyectos.

A continuación se define una descripción a nivel macro de cada a una de las fases así como una concisa definición acerca de los requerimientos requeridos (**E**ntry - Entradas), actividades a ser ejecutadas (**T**ask - Tareas), comprobaciones de calidad a ser ejecutadas (**V**alidation - Validaciones) y definir los entregables establecidos a ser entregados (E**x**it. Salidas). Se centra este tema en proveer validaciones que permitan asegurar el cumplimiento de las actividades definidas para cada fase, así como establecer relaciones del caso que permitan que las salidas de una fase se conviertan en entradas de la sucesiva, para lo cual debe garantizar que la fase anterior haya sido formalmente culminada, esto mediante ejecución de CheckList de validación.

Se presenta a continuación un diagrama de las fases resultantes, expuesto en figura32, en de donde todas ellas poseen relación directa para inicio de la siguiente fase (excepto fase de

Cierre por obvias razones), se expone adicionalmente el conjunto de actividades a ser ejecutadas en monitoreo y control, fase que tiene inter relación a lo largo de la ejecución del resto de fases.

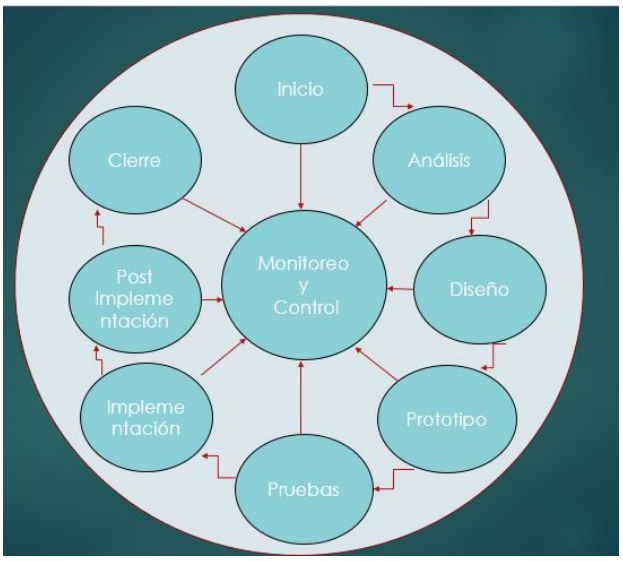

Figura 32. Fases de metodología propuesta.
Fuente: (Erazo, 2016), Elaboración propia

Fase de Inicio

Objetivo Macro

- Crear y definir el caso de negocio, objetivos organizacionales, restricciones, objetivos técnicos en base a requerimientos expuestos y/o iniciativas existentes.

Se expone en la tabla 4 el detalle ETXV propuesto.

Tabla 4. Procesos Fase Inicio

Entradas	Entrega de necesidades o requerimientos (pedido inicial a Alto nivel)
Tareas	• Definir ejecutor y equipo del proyecto • Realizar sesiones de entendimiento con solicitantes por parte de negocio • Definir alcance y presupuesto asignado • Definir objetivos funcionales y técnicos

	• Definir limitaciones técnicas y de negocio • Identificar riesgos • Identificar el alcance de la red • Identificar aplicaciones existentes en la red actual • Identificar políticas internas de seguridad • Cotizar posibles soluciones en base al presupuesto asignado • Definir equipo humano requerido, validar si requiere apoyo externo, proveedores • Crear Gantt inicial con actividades macro
Validaciones	• Formalizar documento final de necesidades y aprobarlo con Responsables de áreas • Definir presupuesto asignado • Cotizar posibles soluciones en base al presupuesto asignado • Formalizar asignaciones de recurso humano • Definir lineamientos con terceros, proveedores • Realizar CheckList de ETVX de fase Creación
Salidas	• Acta de constitución del proyecto • Reunión de kick-off (reunión inicial) • Obtener documento CRD (Customer Requirements Document, documento de requerimientos del cliente) • Definir estrategia de Arquitectura de red • Definir documento caso de negocio • Entrega de Gantt inicial alto Nivel • Entrega de CheckList de ETVX de fase Creación, Ok paso de fase por parte de stakeholders
Monitoreo y control	• Realizar reuniones diarias (15 minutos) con equipo técnico asignado

	• Definir y realizar reuniones semanales con equipo asignado al proyecto (delegados por parte del negocio, ejecutor del proyecto) • Elaborar actas de reuniones realizadas • Obtener aprobación de las áreas involucradas acerca de los riesgos identificados, objetivos plasmados, alcance definido, limitaciones existentes

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

Fase de Análisis

Objetivo Macro

- Examinar los servicios y aplicaciones definidos en el paso anterior y efectuar una validación actual del estado de salud de equipos de la red.

Se expone en la tabla 5 el detalle ETXV propuesto.

Tabla 5. Procesos Fase Análisis

Entradas	• Entrega de ETVX de fase Creación, Ok paso de fase por parte de stakeholders • Documento CRD • Documento de estrategia de Arquitectura derRed • Gantt preliminar • Documento caso de negocio
Tareas	• Definir estado de salud actual de la red y capacity planning • Validar arquitectura de red actual y actualizarla • Definir direccionamiento usado • Definir topología lógica de alto nivel • Validar cableado actual existente, estado del mismo • Realizar diagrama general del cableado existente

	• Realizar POC (Proof of concept, prueba de concepto) • Realizar documento HLD (high level design, diseño de alto nivel) • Realizar diagrama general de la red
Validaciones	• Revisar capacity plannning • Realizar CheckList ETVX de fase Análisis
Salidas	• Estado de salud de la red - Capacity planning • Documento HLD • Definir documento de resultados de POC Gantt detallado • Entrega de CheckList ETVX de fase Análisis, Ok paso de fase por parte de stakeholders
Monitoreo y control	• Realizar reuniones diarias (15 minutos) con equipo técnico asignado • Definir y realizar reuniones semanales con equipo asignado al proyecto (delegados por parte del negocio, ejecutor del proyecto) • Elaborar actas de reuniones realizadas • Brindar seguimiento a riesgos identificados

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

Fase de Diseño

Objetivo Macro

- Definir equipos a ser añadidos o potencializados (de aplicar). Efectuar el diseño de red (actualizarla de aplicar).

Se expone en la tabla 6 el detalle ETXV propuesto.

Tabla 6. Procesos Fase Diseño

Entradas	• Entrega de CheckList ETVX de fase Análisis, Ok paso de fase por parte de stakeholders • Diagrama de topología lógica • Documento HLD (High Level Design, diseño de alto nivel) • Diagrama general de la red • Documento resultados POC
Tareas	• Realizar diagrama detallado de topología y componentes de la red • Definir equipos de redundancia, balanceo de carga • Diseño de red en base a tres capas • Definir esquemas de seguridad • Definir esquemas de direccionamiento • Seleccionar equipos de switching, routing • Definir estrategias de seguridad • Realizar documento SOW (Statement of work, declaración del trabajo) • Efectuar compra de equipos y/o materiales definidos en SOW
Validaciones	• Validar Documento LLD (Low Level design, diseño de bajo nivel) • Obtener compromisos de entrega de equipos • Validar impactos en la red existente • Revisar SOW definido con gerente de TI • Realizar CheckList ETVX de fase Diseño
Salidas	• Documento LLD final • Realizar prueba de verificación del diseño • Definir estrategia final de administración de red • SOW Final a formalizar • Gantt Final

	• Compra de equipos y/o materiales • Entrega de CheckList ETVX de fase Diseño, Ok paso de fase por parte de stakeholders
Monitoreo y control	• Realizar reuniones diarias (15 minutos) con equipo técnico asignado • Definir y realizar reuniones semanales con equipo asignado al proyecto (delegados por parte del negocio, ejecutor del proyecto) • Elaborar actas de reuniones realizadas Brindar seguimiento a riesgos identificados

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

Fase Creación de Prototipo

Objetivo Macro

- Crear la solución diseñada en un ambiente controlado y/o simular el resultado de la solución esperada en base a las especificaciones definidas. En caso de haber existido una POC, varias tareas de esta fase podrían ya haber sido cubiertas y/o podrían ejecutarse en paralelo.

Se expone en la tabla 7 el detalle ETXV propuesto.

Tabla 7. Procesos Fase Creación de Prototipo

Entradas	• Entrega de CheckList ETVX de fase Diseño, Ok paso de fase por parte de stakeholders • Documento LLD • Resultados prueba de verificación • SOW • Evidencia de compra de equipos y/o materiales
Tareas	• Efectuar tareas requeridas para instalación de la solución

	(configuraciones en equipos pre existentes para acoplamiento, instalaciones físicas, requeridas) • Ejecutar implementación de la solución integral en ambiente paralelo (de preferencia crear ambiente de desarrollo o simular mediante herramientas)
Validaciones	• Validar resultados iniciales • Confirmar existencia de instalaciones requeridas • Realizar CheckList ETVX de fase Prototipo
Salidas	• Actualizar documento LLD (de aplicar) • Obtener plan de implementación y plan de roll back (plan de reverso) hacia ambiente de test (o pre producción) • Definir pruebas de funcionalidad, pruebas negativas, pruebas de rendimiento • Entrega de CheckList ETVX de fase Prototipo, Ok paso de fase por parte de stakeholders
Monitoreo y control	• Realizar reuniones diarias (15 minutos) con equipo técnico asignado • Definir y realizar reuniones semanales con equipo asignado al proyecto (delegados por parte del negocio, ejecutor del proyecto) • Elaborar actas de reuniones realizadas Brindar seguimiento a riesgos identificados

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

Pruebas

Objetivo Macro

- Ejecutar pruebas en ambiente de test o pre producción en consideración de las especificaciones existentes y adecuaciones realizadas en fase prototipo (de aplicar)

Se expone en la tabla 8 el detalle ETXV propuesto.

Tabla 8. Procesos Fase Pruebas

Entradas	• Entrega de CheckList ETVX de fase Prototipo, Ok paso de fase por parte de stakeholders • Obtener plan de implementación y roll back
Tareas	• Ejecutar pruebas de funcionalidad • Ejecutar pruebas negativas • Ejecutar pruebas de rendimiento • Ejecutar capacitación a usuarios finales
Validaciones	• Verificar documento de plan de implementación y roll back • Realizar CheckList ETVX de fase Pruebas
Salidas	• Resultados de pruebas (incorporar detalles a considerar) • Plan de implementación y roll back actualizado con datos de ambiente producción • Entrega de CheckList ETVX de fase Pruebas, Ok paso de fase por parte de stakeholders
Monitoreo y control	• Realizar reuniones diarias (15 minutos) con equipo técnico asignado • Definir y realizar reuniones semanales con equipo asignado al proyecto (delegados por parte del negocio, ejecutor del proyecto) • Elaborar actas de reuniones realizadas Brindar seguimiento a riesgos identificados

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

Implementación

Objetivo Macro

- Implementar solución en ambiente de producción en base a información y resultados obtenidos en fase de pruebas

Se expone en la tabla 9 el detalle ETXV propuesto.

Tabla 9. Procesos Fase Implementación

Entradas	• Plan de implementación y roll back a ambiente producción • Entrega de CheckList ETVX de fase Pruebas, Ok paso de fase por parte de stakeholders
Tareas	• Colocar equipos en monitoreo • Definir ventana de mantenimiento • Comunicar el negocio del cambio a realizar y sus posibles implicaciones • Obtener OK de salida a producción
Validaciones	• Checklist de validación de actividades • Ejecución del plan de implementación • Realizar CheckList ETVX de fase Implementación
Salidas	• Informe de resultados obtenidos • Actualizar diagramas de Topología con direccionamiento de nuevos equipos • Entrega de CheckList ETVX de fase Implementación, Ok paso de fase por parte de stakeholders
Monitoreo y control	• Realizar reuniones diarias (15 minutos) con equipo técnico asignado • Definir y realizar reuniones semanales con equipo asignado al proyecto (delegados por parte del negocio, ejecutor del proyecto) • Elaborar actas de reuniones realizadas • Brindar seguimiento a riesgos identificados

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

Post Implementación – Optimización

Objetivo Macro

- Corregir posibles problemas a presentarse, documentar y efectuar la entrega formal de la solución a monitoreo diario.

Se expone en la tabla 10 el detalle ETXV propuesto.

Tabla 10. Procesos Fase Post Implementación - Optimización

Entradas	• Informe de resultados obtenidos • Topología detallada actualizada • Entrega de CheckList ETVX de fase Implementación, Ok paso de fase por parte de stakeholders
Tareas	• Efectuar monitoreo de la solución • Brindar apoyo y solución a problemas presentados • Validar configuraciones de monitoreo de equipo • Crear/actualizar procedimientos de monitoreo de equipos, actualización de firmware, etc.(herramientas existentes)
Validaciones	• Validar documentación de problemas encontrados • Realizar CheckList ETVX de fase Post Implementación
Salidas	• Generar Acta de aceptación final TI • Entrega de documentación generada • Entrega de CheckList ETVX de fase Post Implementación, Ok paso de fase por parte de stakeholders
Monitoreo y control	• Realizar reuniones diarias (15 minutos) con equipo técnico asignado • Definir y realizar reuniones semanales con equipo asignado al proyecto (delegados por parte del negocio, ejecutor del proyecto)

	• Elaborar actas de reuniones realizadas • Brindar seguimiento a riesgos identificados

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

Monitoreo y control

Objetivo Macro

- Brindar apoyo de seguimiento en cada fase del proyecto y especificar actividades de monitoreo propio del proyecto: reuniones, informes de seguimiento, seguimiento de métricas.

Se expone en la tabla 11 el detalle ETXV propuesto.

Tabla 11. Procesos Fase monitoreo y control

Entradas	• Acta de aceptación final TI • Entrega de CheckList ETVX de fase Post Implementación, Ok paso de fase por parte de stakeholders
Tareas	• Establecer procedimientos de monitoreo
Validaciones	• Definir bitácora de monitoreo • Realizar CheckList ETVX de fase Monitoreo y control
Salidas	• Documento definiciones de monitoreo de nueva solución • Entrega de CheckList ETVX de fase monitoreo y control, Ok paso de fase por parte de stakeholders
Monitoreo y control	• Realizar reuniones diarias (15 minutos) con equipo técnico asignado • Definir y realizar reuniones semanales con equipo asignado al proyecto (delegados por parte del negocio, ejecutor del proyecto) • Elaborar actas de reuniones realizadas • Brindar seguimiento a riesgos identificados

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

Cierre

Objetivo Macro

- Formalizar la entrega de la solución y de toda la información recogida a lo largo del ciclo de vida del proyecto.

Se expone en la tabla 12 el detalle ETXV propuesto.

Tabla 12. Procesos Fase Cierre

Entradas	• Validación ok de procesos diarios por 3 días (mínimo) sin errores • Acta de aceptación final TI • Entrega de CheckList ETVX de fase monitoreo y control, Ok paso de fase por parte de stakeholders
Tareas	• Definir mantenimiento de equipos • Definir esquema de licenciamiento
Validaciones	• Realizar Checklist de cierre • Realizar CheckList ETVX de fase Cierre
Salidas	• Acta formal de cierre • Encuesta de satisfacción • Definición de mejores prácticas y lecciones aprendidas • Entrega de CheckList ETVX de fase Cierre, Ok paso de fase por parte de stakeholders
Monitoreo y control	• Elaborar acta final de cierre

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

CAPÍTULO IV

APLICACIÓN DE METODOLOGÍA PROPUESTA MEDIANTE CASO DE ESTUDIO

4.1 Introducción

Una vez definida la propuesta de metodología a ser usada dentro de la institución se procede a implementarla por medio de un caso real solicitado a la interna. En base a las necesidades expuestas para el presente proyecto se expone el desarrollo del mismo teniendo como lineamiento las nueve fases definidas exponiendo para el efecto los entregables principales de cada fase así como toda actividad efectuada para proveer las salidas correspondientes que suelen ser entradas de actividad a realizar en la fase posterior. Denota así ser una metodología de tipo cascada; aun así podría en determinadas situaciones permitir el paralelizar actividades. Es importante puntualizar que el fin del presente trabajo es proveer lineamientos personalizados acorde a la realidad de la institución, apoyando para el efecto en cada una de las metodologías citadas.

4.2 Definición del caso

El caso definido a ser desarrollado responde a una solicitud de la alta gerencia de la institución; cuyo fin es proveer conectividad móvil a usuarios con equipos portátiles y smartphones (teléfonos inteligentes) de tal forma que pueda presentarse mejora en la respuesta de solicitudes a pedidos, a su vez poder brindar nuevos servicios ante el usuario final (cliente interno y externo) mediante la provisión de acceso a Internet. En el caso de usuarios internos busca como beneficio el proveer disminución de costos en provisión de planes celulares y brindar movilidad a los usuarios mientras se encuentran en diferentes lugares del edificio matriz; mientras que para el caso de clientes externos - proveedores tiene como fin brindar acceso a

Internet mientras permanecen en el edificio matriz como un servicio adicional provisto por la institución.

El nacimiento de las necesidades a ser cubiertas en el presente caso se generan a partir de restricciones palpadas por usuarios finales (Altos – medios ejecutivos) quienes al acudir a otras áreas, reuniones; no podían tener acceso a sus archivos y correos causando demora excesiva en respuesta ante temas críticos, adicional de no poseer acceso a aplicaciones internas en tiempo real. Finalmente y a pesar de poseer equipamiento para realización de video conferencias mediante equipos asignados; no se puede tener su uso debido a restricciones de accesos desde otras áreas, salas de reuniones (indisponibilidad de puntos de red).

4.3 Desarrollo del caso

A continuación se ejecutará el desarrollo del caso definido en el punto anterior. Para el efecto se realizará el despliegue del mismo paso a paso a fin de realizar una demostración del uso de la metodología propuesta brindando detalle de los entregables de cada fase con énfasis en aspectos de **redes y comunicaciones.** El fin del presente trabajo es poder proveer una solución que contemple los objetivos técnicos y de negocio y que se ajuste a la provisión de una gestión eficiente de la red con altos niveles de disponibilidad y bajo definiciones de seguridad interna. Adicional de proveer información detallada de los cambios a ser implementados de tal forma que brinde escalabilidad a la red mediante previsión de nuevos servicios y que apoye en la creación / actualización de documentación de la red que permitan proveer mayor disponibilidad, mantener un óptimo monitoreo y permita establecer acciones contingentes ante posibles eventos; adicional de aportar datos ante exigencias de unidades internas de control, así como ante exigencias externas y entes regulatorios.

A continuación el despliegue de la metodología propuesta por el autor ante el caso definido para el efecto.

Es importante puntualizar que por temas de seguridad y confidencialidad se procederá a omitir nombres, direcciones de correo de colaboradores (se definirá por rol); a su vez se considerará variantes en definiciones de direccionamiento de red, topología general, total de agencias, definición de áreas internas del edificio matriz, pisos, ubicaciones, nombres de equipos, etc. Se efectuará sin embargo definiciones propias que permitan al lector mantener una idea del planteamiento original, aun así se proveerá algunas gráficas del resultado obtenido, de igual forma modificando datos reveladores de la topología real.

Entrega de necesidades por parte del solicitante original hacia el área de TI

Para el presente caso, por parte de la alta gerencia se efectúa el pedido de provisión de servicio inalámbrico para personal con equipos móviles (portátiles - Smartphone), adicional de provisión de servicio de Internet (con restricciones) para usuarios externos.

A continuación fiel copia del pedido original (se omiten nombres, direcciones de correo por temas internos [en adelante se citará únicamente como **restricción interna** cuando se deba omitir /cambiar datos internos que no pueden ser evidenciados en el presente documento)

Estimados Tecnología;

Se solicita su gentil ayuda a fin de poder cumplir los siguientes requerimientos en base a acuerdos establecidos en reunión gerencial del 30 de Septiembre 2016:

- Proveer una solución wireless para el edificio matriz considerando 20000 USD de presupuesto y que brinde solución a los siguientes pedidos:

- Establecer una red inalámbrica interna para uso exclusivo de gerentes y personal clave que permita brindar una experiencia de usuario similar a la obtenida al tener conectividad alámbrica.
- Establecer una red inalámbrica para uso de primeras y segundas líneas de supervisión, con accesos restringidos
- Establecer una red inalámbrica para acceso a proveedores y usuarios en general, No deberá tener acceso a la red interna
- Establecer una red inalámbrica para acceso de equipos celulares corporativos con experiencia de usuario similar a una conexión de domicilio (uso simple de clave de acceso)

Desarrollo del proyecto de redes en base a la metodología establecida

A continuación se detalla los resultados obtenidos al aplicar la metodología establecida por el autor; se brinda por la presente un detalle de cada paso efectuado con énfasis en criterios técnicos en lo que respecta a redes y comunicaciones y en base a los entregables de cada fase.

Fase de Inicio

En base al pedido original efectuado por el Solicitante, se procede a identificar los involucrados (stakeholders), aplica **restricción interna**.

Definir equipo del proyecto

Ing. Juan Pablo Moreno (Ejecutor del proyecto)
Ing. David Rincón (Administrador de red)
Ing. Javier Salas (Administrador de red)
Ing. Marcelo Calderón (Soporte técnico/pruebas)
Ing. Daniel Rodas (centro de cómputo)

Ing. Johanna Jara (Recepcionista)

Ing. Daniel Romero (Usuario experto/pruebas)

Ing. Juan Pablo Moreno (Ejecutor del Proyecto)

Ing. Daniel Rosero (Oficial de seguridades)

Ing. Pablo Tirado (Oficial de riesgos)

Ing. Luis López (Sub gerente de tecnología)

Ing. Daniel Coronel (Responsable de marketing)

Dr. Juan Yépez (Sponsor)

Nombre del proyecto

Proyecto_Red_Inalambrica_Edf.Matriz

Presupuesto asignado

20000 USD

Tiempo de implementación

40 días

Durante la semana del 3 al 7 de Octubre 2016 se mantienen sesiones de entendimiento entre los involucrados con fines de acoplar la solicitud realizada por la alta gerencia (representada por Dr. Juan Yépez), adicional de definir el alcance, presupuesto, objetivos técnicos y de negocio, limitaciones, riesgos, cotizaciones, definición de planificación inicial de actividades.

Una vez definidos los parámetros antes expuestos se efectúan las validaciones correspondientes y se definen los siguientes entregables:

Customer Requirements Document (Documento de requerimientos del cliente)

Proyecto_Red_Inalambrica_Edf.Matriz

Octubre 2016

Versión 1.0

*(Documento requiere firmas de los stakeholders)

Aplica **restricción interna**

1. Introducción

El presente documento tiene la finalidad de identificar una línea base de la red implementada en la organización y definir los cambios requeridos (propuestos) para brindar escalabilidad a la red. Adicionalmente tiene por objetivo el definir el alcance de la solución, definir sus posibles riesgos, objetivos técnicos y de negocio en mutuo acuerdo entre el solicitante y el ejecutor.

2. Antecedentes

Se identifica demora excesiva en aprobación de solicitudes por parte de las líneas de supervisión de la institución cuya causa raíz se debe en primera instancia a reuniones internas en donde participa dicho personal clave. La problemática radica en la inexistencia de solución de movilidad que permita al usuario final acceder a la red interna - aplicativo de solicitudes de aprobación de compras desde su equipo portátil; esto al contar con un solo punto de red alámbrico en las salas provistas para dichas reuniones además de imposibilitarse el compartir presentaciones, conferencias. Esta problemática brinda inicio a una necesidad del negocio de ofertar servicio de movilidad al cliente interno – externo

sumándose beneficios y nuevos servicios que parten de este requerimiento inicial y que son requeridos a su vez por parte de la alta gerencia.

3. Alcance

Proveer 4 redes inalámbricas para uso del cliente interno / externo en base a las definiciones expuestas en los requerimientos descritos en el presente documento (sección requerimientos), con apertura a creación de nuevas redes (de ser requerido a futuro).

A nivel técnico y en base a modelo OSI se define alcance a ser cubierto por la solución, expuesto en la tabla 13.

Tabla 13. Alcance de la solución

Alcance del diseño de Red	**Detalle**
red total	Los equipos de comunicaciones de cada piso deben ser revisados a fin de validar disponibilidad de puertos, estado de salud de la red.
Capa de red	Al requerirse nuevos direccionamientos se debe contemplar un nuevo plan de direccionamiento IP (para nuevas redes inalámbricas, no se considera re direccionamiento). Se debe contemplar segmentación y se identifica la necesidad de acoplar nuevo enrutamiento.
Capa enlace de datos	La organización requiere acoplar APs para proveer movilidad a los equipos de usuarios finales. Se requiere validar opciones de implementación para movilidad y alcances de equipos
Capa física	Proveer acceso a punto de red Gigabit para adpación de ls APs en los pisos y provisión de punto de datos Gigabit para el equipo central

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

4. **Supuestos**
    - Existencia de inventario de equipos, IPs, puertos, diseño de red actualizado
    - Contar con configuración de tarjeta inalámbrica de equipos finales de usuarios
    - Contar con punto de datos para los APs a ser colocados en cada piso
    - Enlaces de acceso a Internet ya existentes, solución no contempla costos de provisión de nuevos enlaces
5. **Restricciones**
    - Presupuesto no puede superar los 20000 USD y debe estar listo en 40 días (calendarios)
    - Actividades deben ser ejecutadas durante la jornada laborable, no está autorizado el uso de horas extras
    - Debe contemplarse restricciones de acuerdo a lo establecido para cada red, en base a las definiciones acordadas
    - No deberá exponerse acceso a la red inalámbrica desde ubicaciones de acceso público de clientes (cajas, balcón de servicio, área de crédito)
6. **Riesgos**
    - No poder cumplir la fecha de acuerdo establecido por limitaciones de costo y esfuerzo
    - No poder proveer una solución tecnológica robusta al existir limitaciones de costo y esfuerzo, teniendo impacto directo en la calidad del entregable
7. **Requerimientos del cliente**

A continuación se detalla los requerimientos finales acordados entre las partes, se considera la siguiente tabla de priorización definida en tabla 14, en base a las reuniones mantenidas en conjunto:

Tabla 14. Priorización de requerimientos

Valor	Rating	Descripción
1	Critico	Este requisito es crítico para el éxito del proyecto. El proyecto no será posible sin este requisito.
2	Alto	Este requisito es de alta prioridad, pero el proyecto se puede implementar previo haber cumplido este requisito
3	Medio	Este requisito es algo importante, ya que proporciona un cierto valor, pero el proyecto puede continuar sin él.
4	Bajo	Este es un requisito de baja prioridad, o considerado como: "bueno tener" si el tiempo y el coste lo permiten.
5	A futuro	Este requisito está fuera del ámbito actualmente pero se lo ha incluido aquí por una posible versión futura.

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

1.1 Requerimientos funcionales

En la tabla 15 se exponen los requerimientos provistos por la institución.

Tabla 15. Detalle de requerimientos

Req#	Prioridad	Descripción	Razón fundamental	Usuarios/ Áreas impactadas
General / Base Funcional				
RG-01	1	Crear una red inalámbrica de acceso para la alta gerencia. Deberá contemplar una experiencia de usuario similar a la existente cuando posee conexión LAN, es decir con acceso a la red interna, acceso a Internet sin uso de proxy, acceso a impresoras, Portal interno, correo, FTP, mensajería, aplicativos de uso interno, acceso a cámaras de video vigilancia. Al tener accesos sin restricción debe contar con autenticación por filtrado de dirección MAC (podrá registrarse equipos adicionales: celulares, tablets), control de acceso por medio de Active Directory. Estos accesos deben ser controlados	Proveer acceso a la alta gerencia manteniendo los privilegios existentes al estar conectado a la red LAN	Usuarios de alta gerencia

Req#	Prioridad	Descripción	Razón fundamental	Usuarios/ Áreas impactadas
		por el Oficial de seguridades.		
RG-02	1	Crear una red inalámbrica de acceso para uso de primeras y segundas líneas de supervisión y usuarios con laptop. Deberá contemplar una experiencia de usuario similar a la existente cuando posee conexión LAN, es decir con acceso (limitado) a la red interna, acceso a Internet mediante uso de proxy, acceso al Portal interno, correo, mensajería, aplicativos de uso interno. Al tener accesos a la red interna debe contar con autenticación por filtrado de dirección MAC (listado provisto por área de tecnología de todo equipo portátil suministrado a usuarios de matriz para los usuarios establecidos), control de acceso por medio de Active	Proveer acceso a usuarios con equipos portátiles del edificio matriz, manteniendo las restricciones de acceso a Internet y brindando determinados servicios (no aplica misma experiencia y privilegios existentes obtenidos al poseer conectividad LAN)	Usuarios con equipos portátiles

Req#	Prioridad	Descripción	Razón fundamental	Usuarios/ Áreas impactadas
		Directory. Estos accesos deben ser controlados por el Responsable de tecnología y bajo monitoreo y auditoria del Oficial de seguridades.		
RG-03		Crear una red inalámbrica de acceso para uso de clientes y proveedores. Deberá contemplar una experiencia de usuario similar de tipo guest Access con provisión de acceso mediante clave temporal. Esta red es de uso exclusivo para acceso a Internet sin acceso alguno a la red de datos. Además deberá restringirse el uso de redes sociales, gestores de descarga, acceso remoto, contenido multimedia (YouTube, emisión de radio), acceso muy limitado. La clave de acceso provista deberá ser útil únicamente con	Brindar nuevos servicios a los clientes y proveedores de la institución durante su visita a las instalaciones del edificio matriz, aplica restricciones de uso	Clientes y proveedores

Req#	Prioridad	Descripción	Razón fundamental	Usuarios/ Áreas impactadas
		un equipo y deberá tener periodicidad. Deberá suministrarse un aviso de acuerdo de servicio previo a conectarse a la red, en donde se exponga que el equipo estará siendo monitoreado.		
RG-04	1	Crear una red inalámbrica para uso de equipos celulares de colaboradores que poseen Plan institucional que permita obtener funcionalidad similar a la existente cuando están registrados con su Plan de Internet celular. Se proveerá una clave general para acceso a esta red y será adicionalmente registrada mediante acceso por Mac address (para evitar difusión a usuarios no permitidos)	Disminuir planes celulares de colaboradores según definiciones a aplicar	Usuarios celulares con Plan institucional
RG-05	2	Proveer una solución adaptativa que permita crear	Posibles necesidades	Clientes internos,

Req#	Prioridad	Descripción	Razón fundamental	Usuarios/ Áreas impactadas
		nuevas redes inalámbricas sin impactar las ya existentes	requeridas por el negocio ante una determinada causa	externos, proveedores
Requerimientos de seguridad				
RS-01	1	redes inalámbricas para acceso a usuarios finales no debe tener acceso a la red interna de la institución	Cumplimiento de política de seguridad	Tecnología Riesgos
RS-02	1	Los accesos por medio de uso de Active Directory deben dejar pistas en el sistema a ser implementado a fin de validar que concuerde el acceso del usuario y equipo	La red de inalámbrica para acceso a usuarios finales no debe tener acceso a la red interna de la institución	Tecnología Riesgos
RS-03	1	Las redes no deben ser desplegadas en área de acceso Público, mucho menos donde se brinde servicios de atención de cajas (ingreso/retiro de dineros)	Cumplimiento ley Gubernamental,	Tecnología Riesgos

Req#	Prioridad	Descripción	Razón fundamental	Usuarios/ Áreas impactadas
Requerimientos de monitoreo, Reportes				
RM-01	1	Todo equipo de la solución debe ser incluido en las herramientas de monitoreo de la institución	Continuidad operacional	Centro de cómputo
Requerimientos de auditoria				
RA-01	1	Todo cambio efectuado en las configuraciones debe ser reportado al administrador del centro de cómputo, área de redes, oficial de seguridades, oficial de riesgos	Cumplimiento de política de seguridad	Tecnología Riesgos

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

1.2 Requerimientos no funcionales

En la tabla 16 se exponen los requerimientos no funcionales establecidos.

Tabla 16. Detalle de requerimientos no funcionales

ID	Requerimientos
NFR-001	Las redes inalámbricas deben brindar acceso a 200 usuarios concurrentes y al menos 20 usuarios por AP y permitir escalabilidad para futuro uso o despliegue
NFR-002	Las redes inalámbricas deben estar disponibles durante horarios laborables únicamente

NFR-003	Los APs deben proveer servicio con lata cobertura en áreas donde constan salas de reuniones de los diferentes pisos y oficinas de alta gerencia

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

8. Acuerdos de servicio

Se contempla que el servicio de red wireless a ser provisto no es catalogado como un servicio primario de la institución (en su primera etapa); aun así se aplicarán controles compensatorios como monitoreo de loa access points hasta contar con el presupuesto del caso para proveer contingencia. Si bien no será considerado dentro del documento de SLA existente; se considera la necesidad de mantener un monitoreo permanente de los equipos, contemplar equipos de backup ante posibles fallos (APs).

9. Definición de aplicaciones y servicios requeridos en la nueva solución

a. Aplicaciones requeridas al tener movilidad

En la tabla 17 se detallan las aplicaciones requeridos por la nueva solución.

Tabla 17. Aplicaciones planeadas para nueva solución

Aplicaciones planedas en nueva solución			
Tipo de aplicación	**Aplicación**	**Nivel de importancia (Critico, Importante, No Importante)**	**Observaciones**
E-mail	Microsoft Office Outlook	Critica	
Mensajería – video conferencia	Microsoft Office Lync 2013	Critica	Necesidad de permitir el compartir presentaciones, realizar video conferencias durante sesiones remotas

Aplicaciones planedas en nueva solución			
Tipo de aplicación	**Aplicación**	**Nivel de importancia (Critico, Importante, No Importante)**	**Observaciones**
Navegación	Microsoft Internet Explorer	Importante	Acceso a Internet según privilegios definidos para cada SSID
Herramienta colaborativa	Microsoft SharePoint 2013	Importante	Acceso a Intranet institucional para verificar reportes gerenciales, políticas, procedimientos, manuales
Aplicaciones internas	Control de solicitudes	Critica	

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

b. Servicios requeridos al tener movilidad

En la tabla 18 se detallan los servicios requeridos por la nueva solución.

Tabla 18. Servicios requeridos al tener movilidad

Servicios requeridos	
Servicio	**Observaciones**
Seguridad	Proveer politicas de firewall para proteger la red, acceso a herramienta de deteccion de virus en línea.Uso de autenticación por medio de Active Directory, aplicación de politicas de AD, uso de proxy (de aplicar)
Movilidad	Proveer movilidad a la alta gerencia, empleados, proveedores, clientes

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

10. Objetivos organizacionales

- Brindar servicios de vanguardia
- Reducir costos
- Adicionar nuevas funcionalidades al cliente interno y externo

11. Restricciones organizacionales

- Presupuesto limitado a 20000 USD
- Cumplir políticas internas de acceso y seguridad de la información
- Cumplir con la entrega del pedido original hasta el 11 de Noviembre 2016
- Acatar las regulaciones existentes acerca de inhibidores en lugares de atención al público
- Cumplir normativas existentes

12. Objetivos técnicos

- Modernizar tecnologías obsoletas
- Proveer escalabilidad en la red

13. Restricciones técnicas

- Cumplir políticas internas de seguridad

14. Solución propuesta

Incorporar a la red existente un equipo centralizado para administración de APs a ser colocados en los diferentes pisos del edificio matriz. La solución a ser implementada provee mecanismos de acceso por medio de uso de Active Directory, acceso por Mac address, provisión de direccionamiento con integración con un servidor DHCP. Proveer acceso desde herramientas de monitoreo y administración con soporte SNMP v1, 2, 3. Solución permitirá

escalamiento respecto a aumento de APs, redundancia y balanceo de carga. Además de ajustarse al presupuesto asignado. La solución a implementar será ejecutada a la interna, es decir se define no ser requerido apoyo de personal externo (proveedores), excepto para la POC y su respectiva compra.

Documento de definición de estrategia de Arquitectura de red

Proyecto_Red_Inalambrica_Edf.Matriz

Octubre 2016

Versión 1.0

Aplica **restricción interna**

En base a la documentación existente y levantada por el equipo del proyecto; se tiene las siguientes consideraciones:

Edificio Matriz

Capa core

El data center principal consta dentro de la Infraestructura del edificio matriz, en donde consta el router principal de la institución el mismo que se encuentra conectado al switch principal mediante un puerto Gigabit. Este switch de core esta a su vez conectado hacia los routers de provisión de enlace hacia las agencias de igual forma mediante interfaces gigabit. Existe redundancia de enlace hacia las agencias mediante provisión de HSRP para todo punto y redundancia interna mediante doble provisión de fibra óptica hacia los enlaces provistos por los ISPs tanto para datos como Internet. A este switch de core se extienden switches de distribución hacia los servidores y equipos del data center todos ellos con provisión de puertos

gigabit (vlan1) y conexión hacia los switches de distribución del backbone hacia los diferentes pisos (vlan1), todos ellos con provisión gigabit. Los equipos de comunicaciones usados en esta capa son de marca Cisco.

Capa distribución

Los switches de capa distribución poseen puertos gigabit y se conectan a los switches de acceso mediante uso de patch cords categoría 6a. Se cuenta con equipos marca Cisco y un equipo marca HP.

Capa acceso

Los switches de capa acceso proveen conectividad hacia los equipos finales de usuarios mediante provisión de cableado UTP categoría 6a todos ellos instalados en armarios provistos para cada piso. Los equipos de acceso son de marca HP con provisión de 24 y 48 puertos según el volumen de puertos de datos.

Conectividad Internet

La conexión hacia Internet se la tiene por medio de enlaces provistos por dos distintos ISPs, la provisión de cada enlace pose redundancia de fibra óptica. Los equipos de provisión de Internet forman parte de un clúster de firewall que provee balanceo de carga y redundancia. Se cuenta con equipos Check Point en lo que respecta a equipos firewall.

Agencias

Conectividad hacia agencias

Toda agencia posee conectividad hacia el equipo concentrador de su respectivo ISP; el cual posee una interfaz LAN conectada directamente al switch principal de distribución. Cada

agencia posee redundancia de enlace y se usa HSRP a nivel de LAN. La provisión de Internet se la provee desde la matriz mediante uso de proxy; y mediante salida directa de firewall en casos muy excepcionales. En cada agencia se tiene un rack en el cual constan los equipos de cada proveedor (ruteadores) conectados por medio de enlaces de fibra óptica con doble redundancia, y conexión gigabit hacia un switch de acceso/distribución para conexión hacia equipos finales mediante uso de cableado UTP categoría 6a, de superar 16 estaciones de trabajo consta con switch adicional conectado en cascada.

Caso de negocio

Proyecto_Red_Inalambrica_Edf.Matriz

Octubre 2016

Versión 1.0

*(Documento requiere firmas de los stakeholders)

Aplica **restricción interna**

Resumen ejecutivo

El presente informe provee una evaluación y análisis de costos de las distintas soluciones provistas por los proveedores de la institución que brindaron respuesta a la presente necesidad. Se revela así un detalle de costos del despliegue de la solución así como de la elección realizada en base al cumplimiento de las necesidades provistas como del presupuesto asignado.

Beneficios

- **Flexibilidad**

Mediante movilidad se permite mantener acceso a servicios y recursos de red

- **Incremento de la productividad**

Posibilidad de conexión desde lugares que no se tiene acceso alámbrico

- **Reducción de costos**

Disminución significante del mantenimiento de cableado de red, oportunidad de provisión de acceso a la red sin necesidad de infraestructura cableada. Provisión de Internet en equipos celulares sin necesidad de contemplar planes celulares con provisión de datos y/o disminución del mismo

Problemas

- Mayor análisis en provisión de seguridad para accesos inalámbricos
- Necesidad de nuevos equipos
- Acoplar nuevas configuraciones y dispositivos a la red existente

Dimensionamiento de la solución a alto nivel

La solución a considerar debe contemplar al menos los siguientes parámetros que se exponen en la tabla 19:

Tabla 19. Dimensionamiento de la solución alto nivel

Cantidad/Equipo	Capacidad de usuarios
10 APs	100 usuarios por AP
1 Consola de administración	Soportar 10 APs con posibilidad de

	escalamiento
1 Licenciamiento /Servicio	Provisión de actualizaciones, acceso a soporte en línea, cursos, capacitaciones. Opción similar a Cisco Smart Net

Fuente: (Erazo, 2016), Elaboración en base a metodologías estudiadas

Descripción de los costos

En base a las marcas de equipos usadas se procedió a solicitar propuestas de los diferentes proveedores y apoyo en la implementación en relación a no haber incorporado previamente soluciones inalámbricas. Para el caso se procedió a solicitar cotizaciones de soluciones con equipos Cisco y HP mismo que forman parte de la infraestructura de red de la institución. A su vez se solicitó a los proveedores poder incluir nuevas soluciones; mismas que debían cumplir los siguientes requisitos:

- Proveer soporte y actualizaciones dentro del licenciamiento (de aplicar)
- Dispositivos de red deben proveer protocolo de administración SNMP v1, v2,v3
- Solución del fabricante debe proveer una consola centralizada de administración de la solución
- Proveer equipamiento con SLA de 2-5 días de tiempo de entrega

Problemática existente

Al existir una restricción de costos para la solución a ser contemplada se presenta impacto respecto a soluciones de marcas HP y Cisco, mismas que contemplan solución de primer nivel al ser líderes en estas soluciones, además de contar en cuadrantes de reportes Gardner. A su vez y

al existir una propuesta de otro fabricante por medio de un proveedor calificado se procede a considerarla para la presente selección.

Detalle de costos de las soluciones presentadas

Se recibe dentro del tiempo estipulado cotizaciones de 4 proveedores cuyos valores son los expuestos en la figura 33:

MARCA	AP's	Equipos	Servicio soporte	Instalación	TOTAL		Frec	Control Server
CISCO	15	$ 43,875.63	$ 4,512.16	$ 5,000.00	$ 53,387.63	new	2.4GHz	Requerido ISE NAC & ACS application
HP	15	$ 43,583.00	$ 4,600.00	$ 0.00	$ 48,183.00	new	2.4GHz	Requerido HP IMS PLATFORM
CISCO	15	$ 23,994.41	$ 2,815.23	$ 3,500.00	$ 30,309.64	new	2.4GHz	Requerido ISE NAC & ACS application
RUCKUS	10	$ 9,491.50	$ 650.00	$ 0.00	$ 10,141.50		2.4 y 5 GHz	no requiere, embebido en el controlador

Figura 33. Detalle de costos.
Fuente: (Erazo, 2016), Elaboración propia en base a cotizaciones de proveedores

Se consultó adicionalmente posible provisión de solución en calidad de Renta de equipos; para el efecto se visionó servicio contemplado a tres años con los siguientes resultados, expuestos en figura 34.

MARCA	AP's	Instalación	RENTA MENSUAL		VALOR EN 3 AÑOS
CISCO	15	$5,000.00	$3,222.54	contrato 3 años	$116,011.44
CISCO	15	$3,500.00	$2,473.40	contrato 2 años	$89,042.40
CISCO	15	$3,500.00	$2,255.78	contrato 3 años	$81,208.08
CISCO	15	$3,900.00	$2,023.00	contrato 3 años	$72,828.00

Figura 34. Detalle de costos-renta.
Fuente: (Erazo, 2016), Elaboración propia en base a cotizaciones de proveedores

Solución propuesta

En base a las reuniones de trabajo realizadas con el equipo del proyecto y altas gerencias y ante las bondades provistas por la solución de fabricante Ruckus se decide en conjunto el optar

por esta solución, siendo clara la necesidad de efectuar una prueba de concepto previo a su implementación, a fin de garantizar el cumplimiento de los aspectos propuestos. Para el efecto el proveedor finalista expone los siguientes costos; proforma con caducidad a quince días:

1 Ruckus Zone Director 1200 $ 2265,00 + IVA

15 ZoneFlex R710 $ 9750,00 + IVA

Licenciamiento, soporte (1 año) $ 650 + IVA

Total **$ 12665 + IVA**

Tiempo de entrega 1 día

Gantt preliminar, expuesto en figura 35

Nombre de tarea	Duración	Comienzo	Fin	Costo
Proyecto Red WiFi	**26 días**	**3/10/16**	**11/11/16**	**$20,000.00**
PROYECTO RED WIF	**26 días**	**3/10/16**	**11/11/16**	**$20,000.00**
Inicio	4 días	3/10/16	7/10/16	$0.00
Analisis	4 días	7/10/16	13/10/16	$0.00
Diseño	**5 días**	**13/10/16**	**20/10/16**	**$20,000.00**
Compra de eq	5 días	13/10/16	20/10/16	$20,000.00
Creación de Proto	4 días	13/10/16	19/10/16	$0.00
Pruebas	3 días	19/10/16	24/10/16	$0.00
Implementación	2 días	24/10/16	26/10/16	$0.00
Post Implementac	3 días	26/10/16	31/10/16	$0.00
Monitoreo y Contr	5 días	31/10/16	10/11/16	$0.00
Cierre	1 día	10/11/16	11/11/16	$0.00

Figura 35. Gantt preliminar.
Fuente: (Erazo, 2016), Herramienta Project 2010, Elaboración propia

Fase de Análisis

Estado de salud de la red – capacity planning

En base a las herramientas de administración de red existentes en la institución se logra evidenciar la existencia de 1 ruteador (Gateway interno), 6 ruteadores (concentrador ISP1 (red datos hacia agencias), concentrador ISP2 (red de datos hacia agencias), concentrador de filiales y cadenas, Internet ISP1, Internet ISP2, 1 ruteador DHCP Server para telefonía IP), 6 switches administrables Cisco, 20 switches administrables marca HP), 2 equipos UTM Check Point (clúster), 1 IDS, 2 firewall Cisco. No se cuenta con equipo alguno de aprovisionamiento wireless. En lo que respecta a routers y switches Cisco se valida el contar con la última versión de IOS disponible, adicional de no presentarse problema alguno de uso excesivo de CPU, memoria, pérdida de paquetes. Adicional se efectúa un inventario de puertos con fines de validar disponibilidad de puertos. Cabe mencionar apenas hace un mes atrás de la presente implementación se ejecutó actividades de mantenimiento en los equipos de comunicaciones así como actualización de equipos obsoletos en la capa de acceso y distribución, se identifica colocar 3 switches adicionales.

Se verifica tener redundancia desde y hacia las diferentes agencias al existir dos concentradores que proveen la conectividad matriz-sitio remoto (agencia). Se verifica existir redundancia a nivel de salida a Internet (mediante clúster de firewall) con aprovisionamiento de IPs públicas con cada ISP y para cada servicio (correo electrónico, SFTP, servidores Web. Se identifica adicionalmente la existencia de un IDS y un firewall interno colocado en el core y un firewall para provisión de acceso hacia filiales y cadenas.

Se identifica el uso de varias VLANs; vlan1 (equipos matriz), vlan2 (telefonía IP). No se cuenta con políticas de QoS. Se identifica el uso de varias redes secundarias creadas en el Gateway principal interno.

Se cuenta con acceso remoto mediante VPN provista por medio del clúster de firewall.

Se adjunta algunas capturas de los principales equipos de la red; en los repositorios del proyecto se adjunta a detalle las estadísticas validadas en cada equipo.

Por temas de confidencialidad y seguridad no se puede proveer detalles adicionales.

Router interno

Uso de CPU (promedio 8%, pico máximo de 20%, expuesto en figura 36, 37).

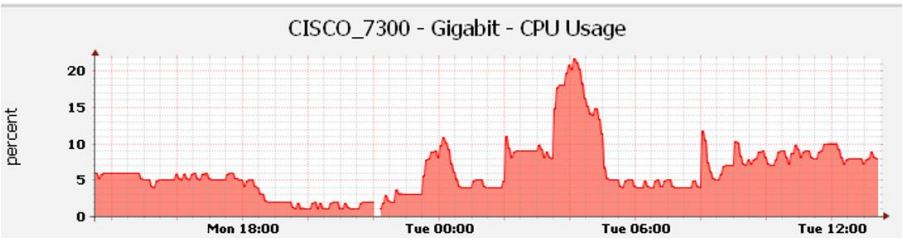

Figura 36. Uso CPU Router.
Fuente: (Erazo, 2016), Herramienta Cacti, Elaboración propia

```
BS_GW#sh proce
CPU utilization for five seconds: 8%/6%; one minute: 8%; five minutes: 8%
 PID QTy       PC Runtime (ms)    Invoked   uSecs    Stacks TTY Process
   1 Cwe 6097DA30           0         53       0 5488/6000   0 Chunk Manager
   2 Csp 60958110         252     555519       0 2556/3000   0 Load Meter
   3 Mwe 626B8344           0          1       0 5572/6000   0 chkpt message ha
   4 Mwe 61A4C160           4          1  400023384/24000   0 EDDRI_MAIN
   5 Lst 6097AD84      928812     283650    3274 5264/6000   0 Check heaps
   6 Cwe 60982F88       11768      28080     419 5440/6000   0 Pool Manager
   7 Mst 6081823C           0          2       0 5520/6000   0 Timers
   8 Mwe 600232F4           0          2       0 5516/6000   0 Serial Backgroun
   9 Mwe 6028B858           0          2       0 5516/6000   0 ATM Idle Timer
  10 Mwe 603122FC           0          2       0 8520/9000   0 ATM AutoVC Perio
  11 Mwe 60311D60           0          2       0 5520/6000   0 ATM VC Auto Crea
  12 Mwe 607D3A28           0          2       0 5508/6000   0 AAA high-capacit
  13 Lwe 607D8AF0           0          1       0 5736/6000   0 AAA_SERVER_DEADT
  14 Mwe 6083F3FC           0          1       011540/12000  0 Policy Manager
  15 Mwe 6089D988           0          1       023476/24000  0 Crash writer
  16 Mwe 60925ECC           0          1       0 5724/6000   0 RO Notify Timers
  17 Msi 60A638A4      728360    2780202     261 5520/6000   0 EnvMon
  18 Mwe 60A6AA18           0          1       0 8560/9000   0 OIR Handler
  19 Mwe 60A874DC           0      46294       0 5668/6000   0 IPC Dynamic Cach
  20 Mwe 60A7B9F8           0          1       0 5592/6000   0 IPC Zone Manager
  21 Mwe 60A7B538          12    2777466       0 5704/6000   0 IPC Periodic Tim
  22 Mwe 60A7B3D8          20    2777467       0 5568/6000   0 IPC Deferred Por
  23 Mwe 60A7B738           0          1       0 5532/6000   0 IPC Seat Manager
  24 Mwe 60A7EC2C           0          1       0 5596/6000   0 IPC BackPressure
```

Figura 37. Uso CPU Router
Fuente: (Erazo, 2016), Elaboración propia

Uso de memoria, expuesto en figura 38

```
BS_GW#       sh memory
                 Head    Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)
Processor   64B73D40   155763164    24312436   131450728   130862792   122208732
      I/O   E000000     33554432     3843544    29710888    29492432    29342332
```

Figura 38. Uso de memoria Router
Fuente: (Erazo, 2016), Elaboración propia

Switch de core (uso de CPU y memoria), expuesto en figura 39

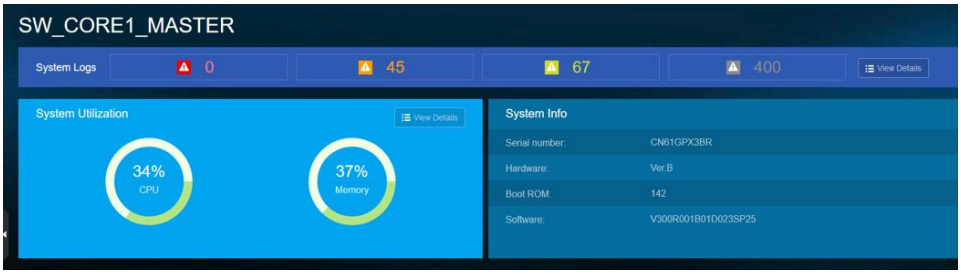

Figura 39. Uso de CPU y memoria Switch Core
Fuente: (Erazo, 2016), Herramienta HP, Elaboración propia

Tráfico switch core, expuesto en figura 40

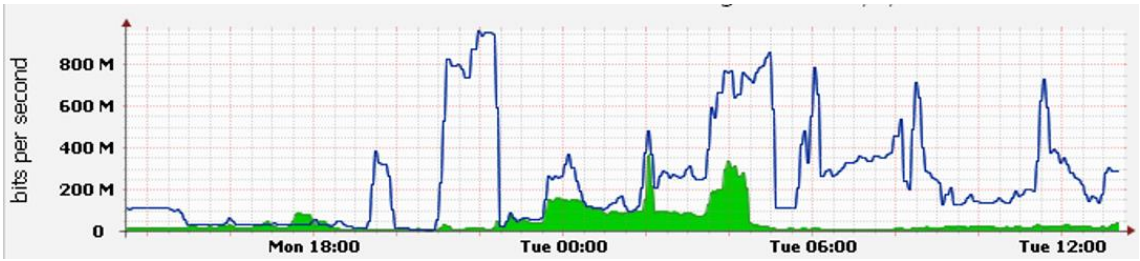

Figura 40. Tráfico switch core
Fuente: (Erazo, 2016), Herramienta Cacti, Elaboración propia

Tráfico Internet ISP 1, expuesto en figura 41

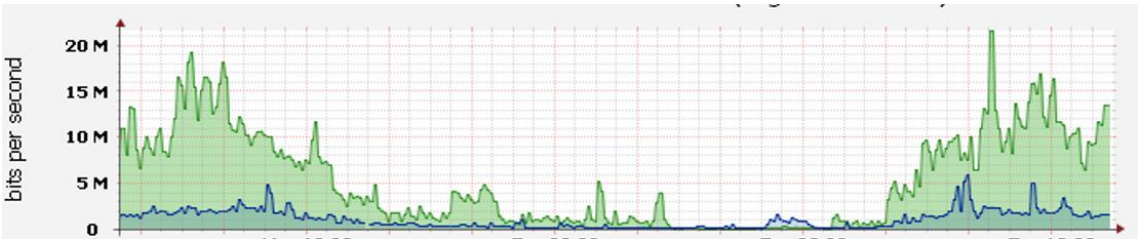

Figura 41. Tráfico enlace Internet
Fuente: (Erazo, 2016), Herramienta Cacti, Elaboración propia

El esquema de direccionamiento IP responde a los siguientes rangos (restricción interna), expuesto en tabla 20:

Tabla 20. Esquema de direccionamiento IP

Asignación subredes IP	
Subred	**Asignación**
10.0.200.0/21	Equipos matriz
10.0.230.0/24 10.0.231.0/24	Redes secundarias matriz
10.0.208.0/24	Impresoras, cámaras matriz
172.16.20.0/23	Telefonía IP matriz
10.200.1.0/19	Agencias(Constan dentro del rango) 10.200.0.1/24 Suc1_Quito 10.200.1.1/24 Suc2_Quito 10.200.2.1/24 Suc3_Quito 10.200.3.1/24 Suc4_Quito 10.200.4.1/24 Suc5_Quito 10.200.5.1/24 Suc6_Quito 10.200.6.1/24 Su7_Quito 10.200.7.1/24 Suc8_Quito

Asignación subredes IP	
Subred	**Asignación**
	10.200.8.1/24 Suc9_Quito 10.200.9.1/24 Suc10_Quito 10.200.10.1/24 Suc1_Guayaquil 10.200.11.1/24 Suc2_Guayaquil 10.200.12.1/24 Suc3_Guayaquil 10.200.13.1/24 Suc4_Guayaquil 10.200.14.1/24 Suc5_Guayaquil 10.200.15.1/24 Suc_Tulcan 10.200.16.1/24 Suc_Ibarra 10.200.17.1/24 Suc_Otavalo 10.200.18.1/24 Suc_Cayambe 10.200.19.1/24 Suc_Santo Domingo1 10.200.20.1/24 Suc_Santo Domingo2 10.200.21.1/24 Suc_Quevedo 10.200.22.1/24 Suc_Esmeraldas 10.200.23.1/24 Suc_Manta 10.200.24.1/24 Suc_Latacunga 10.200.25.1/24 Suc_Ambato1

Asignación subredes IP	
Subred	**Asignación**
	10.200.26.1/24 Suc_Ambato2 10.200.27.1/24 Suc_Riobamba 10.200.28.1/24 Suc_Cuenca1 10.200.29.1/24 Suc_Cuenca2 10.200.30.1/24 Suc_Cuenca3 10.200.31.1/24 Suc_Lago Agrio
Telefonía IP agencias	172.16.1.0/20 constan dentro del rango especificado

Fuente: (Erazo, 2016), Elaboración propia

Toda red de agencias posee como estándar el usar la primera dirección útil como Gateway y las dos siguientes direcciones como Gateway para cada proveedor. Se usa adicionalmente aprovisionamiento DHCP (provisto por servidor de agencia) con direccionamiento 10.200.x.30 al 10.200.x.180, el servidor de agencia posee la última dirección útil (10.200.x.254). El rango para impresoras esta entre el 10.200.x.181 – 10.200.x.200; el rango para cámaras consta desde el 10.200.x.201 al 10.200.x.220

Ejemplo:

HSRP_Gateway 10.200.31.1

HSRP_ISP_1 10.200.31.2

HSRP_ISP_1 10.200.31.3

DHCP_Lago_Agrio (equipos de usuario) 10.200.31.30 -10.200.31.180

Servidor agencia 10.200.31.254

Impresoras (10.200.31.181 – 10.200.31.200)

Cámaras (10.200.31-201 – 10.200.31.220)

Todo equipo interno y de proveedores consta con una comunidad SNMP y permisos para monitoreo desde equipo asignados de monitoreo ubicados en matriz. Se cuenta con acceso de lectura a equipos de proveedor mediante uso de ssh y se tiene configurado el comando **ip accounting output-packets** con la finalidad de validar uso de ancho de banda desde los equipos internos y validaciones básicas ante posibles problemas. Los privilegios para comandos son:

privilege exec level 7 traceroute

privilege exec level 7 ping

privilege exec level 7 show version

privilege exec level 7 show interfaces

privilege exec level 7 show startup-config

privilege exec level 7 show running-config

privilege exec level 7 show

Una vez validados todos los equipos de comunicaciones internos y de proveedor se alerta las siguientes consideraciones:

- Se requiere colocar un switch adicional en los pisos 2 y 8 debido a que el consumo de puertos supera el 90%; tema similar se encuentra en las agencias Quito2, Quito4, Guayaquil1, Guayaquil2, Cuenca1, Ibarra, Santo Domingo y Manta (agencias Quito2 y Santo Domingo poseen uso de puertos al 100%)
- Se requiere crear puntos de datos para los equipos wireless a ser implementados
- No se detecta problema alguno de versiones de IOS de equipos Cisco y actualizaciones en equipos HP están al día
- Se mantiene respaldo de toda configuración de equipos en los repositorios correspondientes
- El uso de CPU, memoria y enlace de los dispositivos en ninguno de los casos supera el 40%
- Se ha obtenido a detalle el listado de puertos disponible en cada equipo de comunicaciones
- Se identifica la necesidad de subir la capacidad del enlace de Lago Agrio a 1 Mega, al momento solo posee enlace de 512, evidenciándose existir consumo superior al 70%, se identifica necesidad de actualizar el equipo (obsoleto)

Documento HLD

Aplica **restricción interna**

Introducción

El presente documento tiene como fin el definir los equipos y tecnologías elegidos para brindar solución al proyecto y cumplir los objetivos técnicos y de negocio. Adicional brinda una

panorámica de la red actual existente y los cambios a alto nivel requeridos para incorporar la nueva solución. Contempla adicionalmente equipos y tecnologías elegidos para cumplir objetivos técnicos y de negocio. Se detalla adicionalmente la topología a nivel general, diagramas de red (disposición de equipos y conexiones de capa física).

Red actual

A nivel macro la red de la institución posee el siguiente la siguiente visión modular, ilustrada en figura 42:

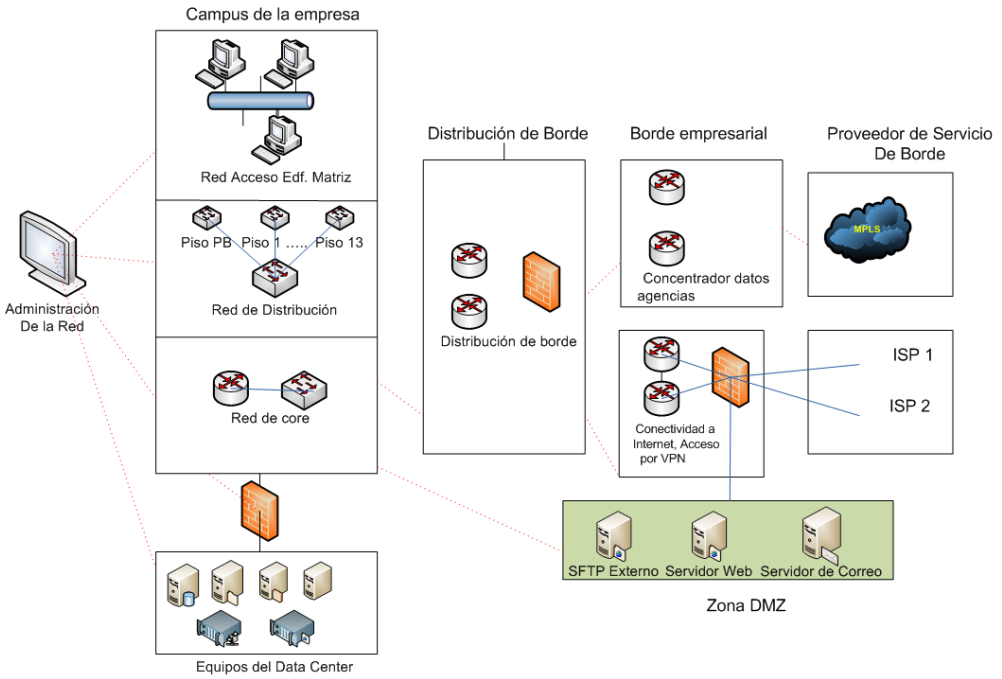

Figura 42. Vista modular
Fuente: (Erazo, 2016), Herramienta Visio 2010, Elaboración propia

En cuanto al cableado se refiere; en el edificio matriz se tiene el siguiente esquema de cableado ilustrado en figura 43, consta de PB, Mezanine 1 y 2 y Pisos 1 al 12, en cada piso se contempla el uso de cableado UTP categoría 6a tanto en la distribución horizontal como vertical. Se evidencia un trabajo reciente de re estructuración del cableado de cada piso debido a mejoras

y cambios en cada uno de ellos. Se identifica una correcta nomenclatura de cada punto de red tanto en el armario de comunicaciones como en cada punto de acceso final de usuario.

Figura 43. Cableado general
Fuente: (Erazo, 2016), Herramienta Visio 2010, Elaboración propia

En lo que respecta a agencias se tiene como estándar el siguiente esquema de cableado ilustrado en figura 44, en donde constan los equipos principales (router, switch, servidor de agencia, DVR) dentro del armario de comunicaciones y se despliega todo punto de red de la

edificación por medio de cableado 6a. Toda agencia posee correctamente la nomenclatura de cableado.

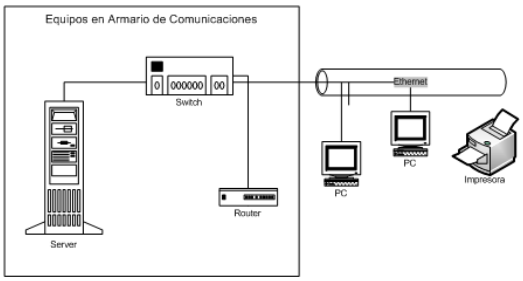

Figura 44. Esquema agencias
Fuente: (Erazo, 2016), Herramienta Visio 2010, Elaboración propia

A continuación se presenta en la figura 45 la topología general de red en cuanto a la matriz y sus 32 agencias a nivel nacional

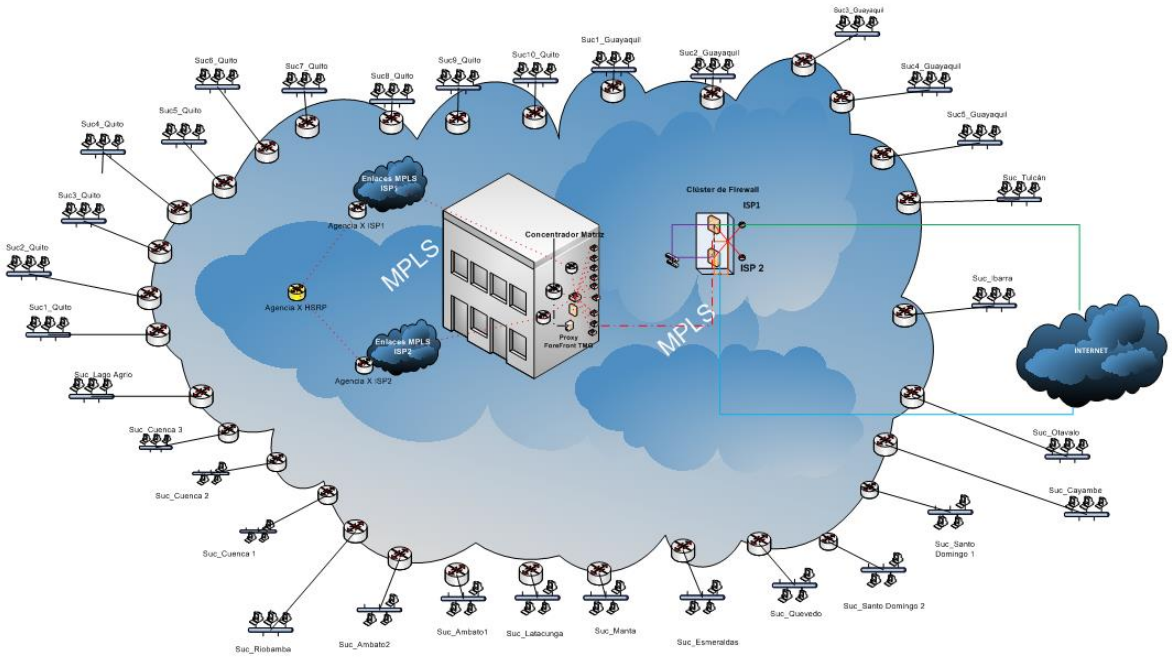

Figura 45. Topología general de la red
Fuente: (Erazo, 2016), Herramienta Visio 2010, Elaboración propia

A su vez el despliegue general jerárquico de la topología del edificio central en donde se identifica requerirse cambios para considerar el nuevo equipamiento y la solución correspondiente. A nivel general se cuenta con la siguiente topología, figura 46:

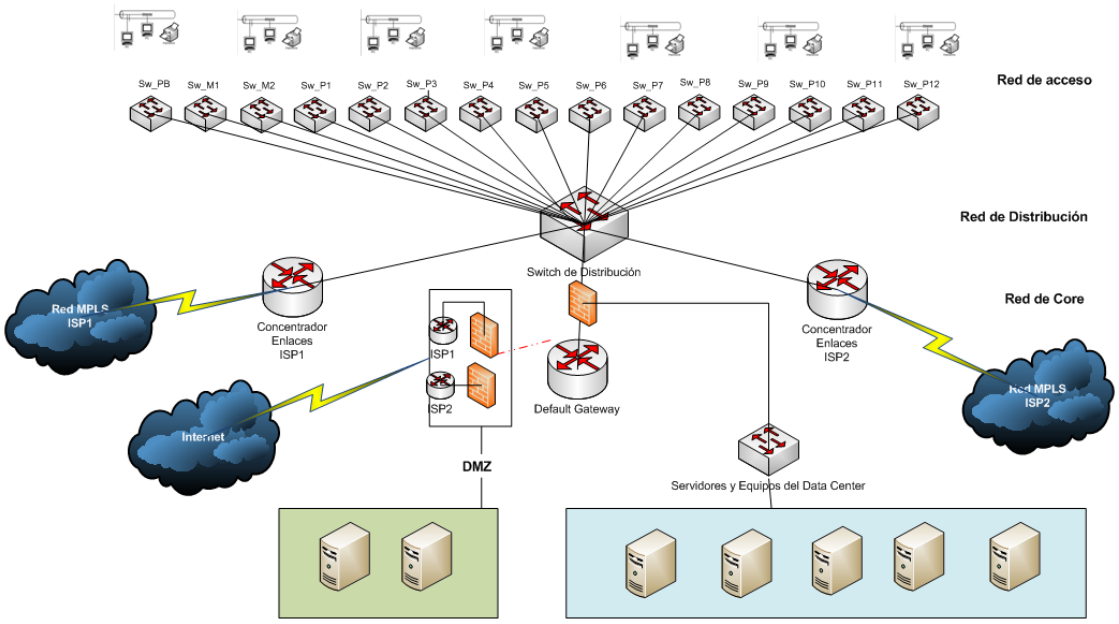

Figura 46. Despliegue jerárquico de la red
Fuente: (Erazo, 2016), Herramienta Visio 2010, Elaboración propia

Equipamiento propuesto

La solución contempla el uso de un equipo centralizado de administración de las WLANs así como de los APs a ser considerados en cada equipo (donde aplique).En términos generales los equipos poseen las siguientes características:

Zone Director 1200

- Permite administrar hasta 256 WLANs, 75 APs y hasta 2000 clientes
- Uso de protocolo de administración SNMP v3

- Soporta autenticación 802.1x, guste access, Active Directory, RADIUS, LDAP
- Soporta control de acceso, soporte a estándares 802.11.x

ZoneFlex R710

- Uso de antena adaptativa y mitigación de interferencia de forma automática
- Posibilidad de uso de acceso de tipo guest access, Hotspot, acceso LDAP, Directorio Activo y Radius
- Uso por medio de consola de administración centralizada y posibilidad de uso de tipo standalone
- Uso de MU-MIMO 4*4:4
- Posibilidad de albergar más de 500 usuarios concurrentes por AP
- Posibilidad de entrega de tasa de hasta 1.7 Gbps en banda 5GHz y hasta 800 Mbps en banda 2.4 GHz

En base a las características expuestas de los equipos se defines los siguientes requerimientos y consideraciones a tomar en cuenta:

Requerimientos generales a considerar

- Validar las WLAN a ser colocadas en cada piso donde será implementado
- Crear puntos de red y definir ubicación de cada AP a ser colocado por piso
- Verificar opciones para direccionamiento DHCP para cada WLAN
- Validar consideraciones de Active Directory, respecto a políticas de red, definición de sites

Cambios a considerar

- Crear sites en Active Directory para las nuevas redes que usarán acceso mediante LDAP
- Crear DHCP scope para redes a ser configuradas con Active Directory
- Adicionar red que usará proxy dentro del equipo Forefront (adicionar subred)
- Crear objeto red LAN en firewall Check Point para salida directa a Internet
- Crear restricciones en firewall interno para asegurar que red de acceso de clientes no posea acceso alguno a la red interna de datos
- Configurar puerto de switch de acceso de cada piso en VLAN1
- Crear ruta de nuevas redes en equipo clúster de firewall Check Point
- Realizar Acta de ingreso de equipos nuevos al Data Center

Consideraciones de seguridad y privacidad

- Enjaular cada red WLAN de tal forma que no pueda efectuarse descubrimiento de equipos
- Habilitar filtrado de MAC Address para redes que proveen acceso a la red interna, adicional de realizar acceso por medio de Active Directory
- Verificar la imposibilidad de acceso desde instalaciones del edificio que brindar acceso público de clientes
- Establecer nombres de redes WLAN que no den pista alguna del origen institucional a la que pertenecen
- Mantener pista de auditoria de accesos, habilitación de permisos

- Definir roles de uso en la herramienta de Administración: administrador de red, Creador de accesos tipo guest, acceso para oficial de seguridades

Requerimientos de disponibilidad

- Garantizar disponibilidad de las WLAN solamente en horarios de trabajo
- Mantener monitoreo de los equipos a ser colocados en los diferentes pisos
- Mantener configuraciones de tal forma que se habilite equipo de contingencia ante posible fallo

Expectativas de volumen y desempeño

- Permitir acceso al menos a 20 usuarios por AP con posibilidad de crecimiento a futuro de al menos el 100% adicional
- Colocar reglas que permitan brindar conectividad de alto ancho de banda en red de alta gerencia

Requerimientos de conectividad

- Poseer un puerto libre en el switch de acceso de cada piso configurado con acceso a VLAN requerida
- Proveer un puerto en el switch de core para habilitar consola de administración general
- Brindar acceso a las WLAN determinadas para uso en cada piso
- Obtener información de la dirección Mac address de los equipos móviles

Integración con red actual

En la figura 47 se expone el diagrama de integración de los equipos provistos con la nueva solución y la ya existente.

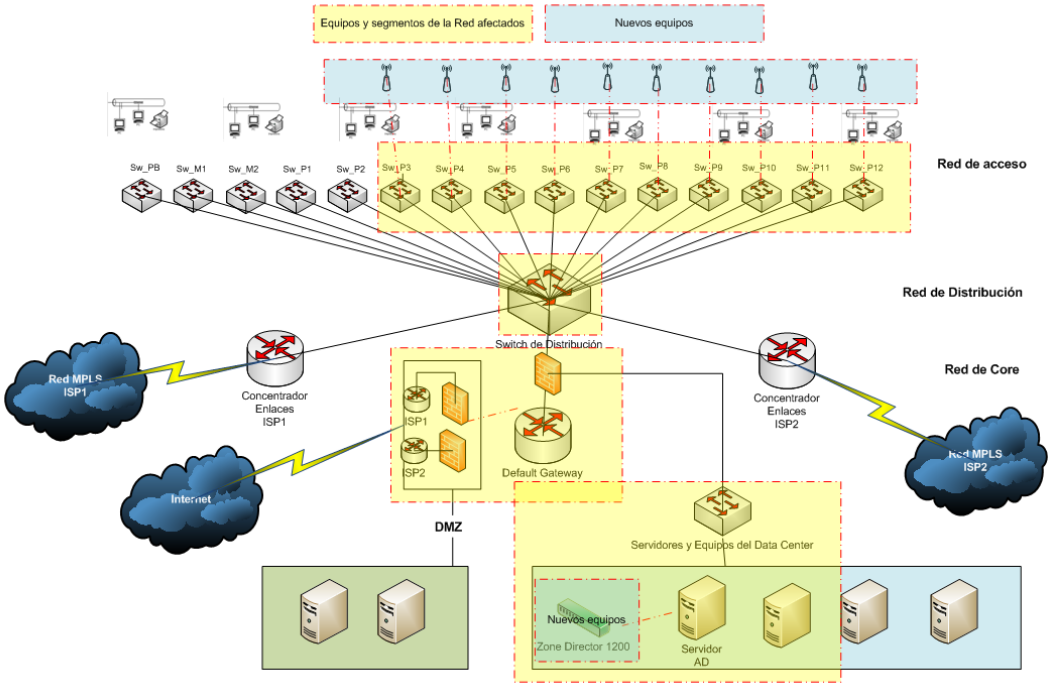

Figura 47. Integración de la red con nuevos equipos
Fuente: (Erazo, 2016), Herramienta Visio 2010, Elaboración propia

Impactos operacionales

- Definir usuario responsable por piso a quien pueda el cliente externo solicitar su acceso de tipo guest access
- Definir usuario auditor que valide equipos con accesos a red interna (con y sin proxy)
- Definir bitácora de monitoreo e incluir nuevos equipos en herramientas de monitoreo a cargo del área de centro de cómputo

Impactos organizacionales

- Crear cultura de concientización de uso de red inalámbrica a usuarios, proveedores y clientes
- Incorporar procesos institucionales y acoplar a existentes impactados

- Ofertar nuevo servicio al cliente interno y externo con apoyo del área de marketing (crear señales de aviso de zona WiFi en los pisos)

Riesgos

- No contar con respaldo de administradores de la herramienta ante restricciones de acceso a personal no autorizado
- No contar con las restricciones necesarias que permitan acceso no autorizado desde equipos externos
- No contar con soporte a largo plazo con equipamiento de la solución elegida
- No contar con segmentación de Subredes por área interna
- No contar con aceptación por parte de la alta gerencia ante restricciones para acceso de nuevos equipos

Documento de resultados de POC

Introducción

La presente prueba de concepto permitirá efectuar un ejercicio previo a la implementación de la solución de tal forma que permita validar sus funcionalidades y permita acoplar de mejor forma el diseño requerido para su óptimo funcionamiento.

Alcance de la POC

Se limita a la validación de las 4 redes WLANs provistas como solución el pedido de la alta gerencia y cumplimiento de las especificaciones determinadas para cada una de ellas. Para el efecto de la POC el proveedor ha suministrado 4 equipos:

- 1 equipo Zone Director 1200 para administración centralizada de la solución

- 3 APs para simular conectividad desde 3 pisos

Con estas consideraciones; las pruebas se limitan a verificar el uso desde 3 pisos y validar toda configuración, administración y monitoreo desde el equipo de administración central a ser considerado en la solución integral.

Detalle de la prueba de concepto

Una vez provistos los equipos y validada la documentación de los mismos; se procede con la configuración inicial del equipo de administración general Zone Director, al cual se coloca en la subred existente con direccionamiento DHCP provisto por VLAN 112.

Siguiendo configuraciones iniciales del equipo se adjunta un usuario y clave de administrador. Cumpliendo con requerimientos internos el acceso de tipo Web a la consola de administración usa protocolo HTTPS, tal y como se evidencia en la figura 48:

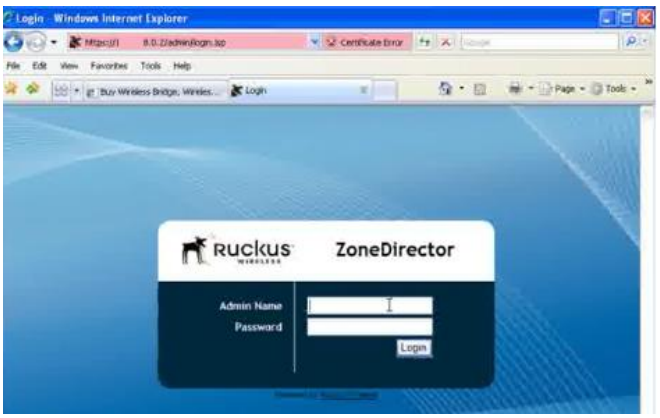

Figura 48. Acceso Web a Consola Ruckus
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Se valida que al colocar un nuevo equipo AP posee el equipo de administración la opción de auto adherirlo a la Consola; para el efecto con una IP correspondiente al DHCP general de la VLAN112 de desarrollo (192.168.102.0/24).

Una vez integrados los equipos APs a la consola de administración con configuraciones por defecto; se procede a configurar la subred de desarrollo en el firewall que provee salida directa a Internet, adicional se coloca accesos hacia equipos de producción para validar navegación por proxy, uso de correo, administración del agente antivirus (se adjunta formulario de reglas de firewall, access list). Al existir conectividad a Internet y hacia equipos de la red interna y con fines de seguridad se coloca los ESSID en status oculto):

Red alta gerencia

Se coloca el nombre de la WLAN y del ESSID como **RG-01** manteniendo trazabilidad con su requerimiento funcional. Según definición se contempla accesos a toda la red de datos e Internet sin restricciones y se contempla el uso de autenticación por medio de Mac address, adicional de acceso por Directorio Activo.

Tipo de uso WLAN: Standard Usage, tal y como se ilustra en figura 49.

Figura 49. Tipo WLAN para RG-01
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Método de autenticación: Mac Address, encripción WPA-Mixed con algoritmo de tipo Automático y frase de acceso: 65*%$HgdA, tal y como se ilustra en figura 50.

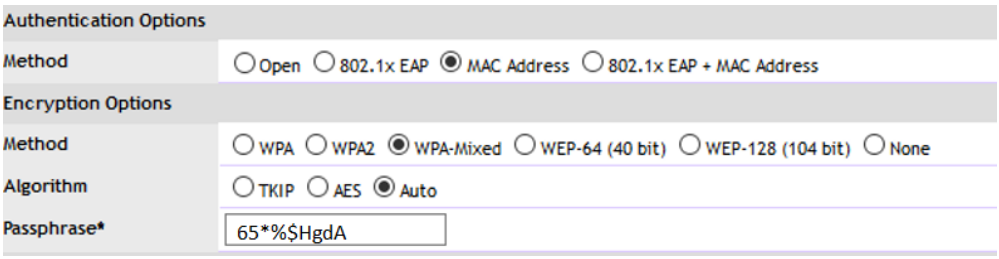

Figura 50. Autenticación y encripción para RG-01
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Generación de direccionamiento IP mediante uso de DHCP Server de Windows 2008 R2 ambiente desarrollo, con provisión de direccionamiento en subred 192.168.102.0/24, se ilustra en figura 51.

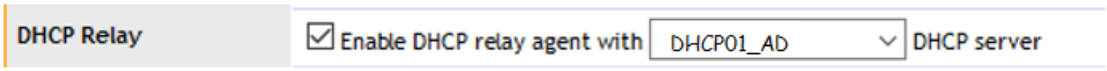

Figura 51. Configuración DHCP para RG-01
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Adicional autenticación por medio de Active Directory y enjaulamiento en la subred definida sin poder ser visto desde otras WLANs y desde clientes de la misma WLAN, se ilustra en figura 52.

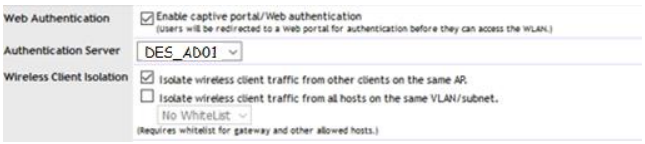

Figura 52. Autenticación Active Directory para RG-01
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Colocar alta prioridad ante otras WLANs, tal y como se ilustra en figura 53.

Figura 53. Opción de prioridad RG-01
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Ocultar el SSID, tal y como se ilustra en figura 54.

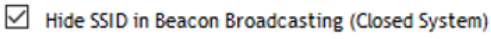

Figura 54. Ocultar SSID para RG-01
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Definir una tasa límite de uso de AB, se ilustra en figura 55.

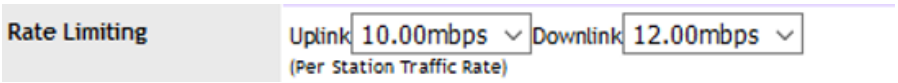

Figura 55. Tasa límite Uso de AB para RG-01
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

No solicitar a menudo el ingreso de clave, se ilustra en figura 56.

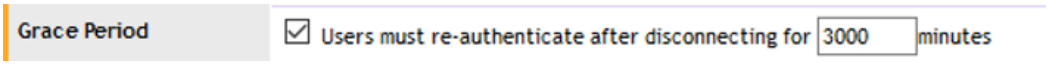

Figura 56. Tiempo para re autenticación para RG-01
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Mantener trazabilidad de toda acción del cliente, se ilustra en figura 57.

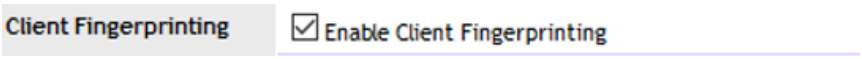

Figura 57. Obtener logs de conexión en red RG-01
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

La red debe estar disponible en horario definido, se ilustra en figura 58.

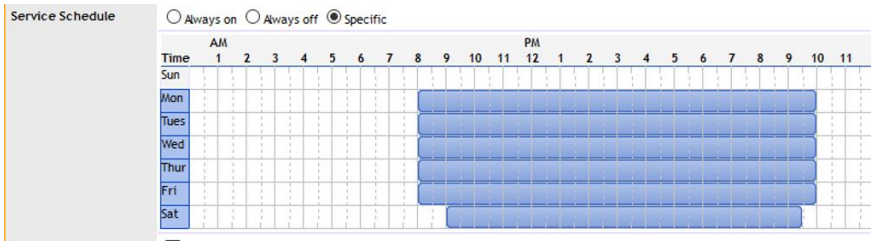

Figura 58. Horario de habilitación red RG-01
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Red líneas de supervisión y usuarios Laptop

Se coloca el nombre de la WLAN y del ESSID como **RG-02** manteniendo trazabilidad con su requerimiento funcional. Según definición se contempla accesos la red interna (acceso con limitaciones) e Internet con uso de proxy (se adjunta detalle de configuraciones requeridas para provisión de Internet mediante proxy) y se contempla el uso de autenticación por medio de Mac address, adicional de acceso por Directorio Activo.

Tipo de uso WLAN: Estándar Usage, se ilustra en figura 59.

Figura 59. Tipo WLAN para RG-02
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Método de autenticación: Mac Address, encripción WPA-Mixed con algoritmo de tipo Automático y frase de acceso: super.37, se ilustra en figura 60.

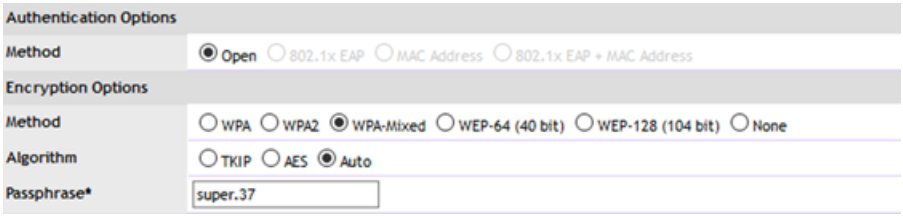

Figura 60. Autenticación y encripción para RG-02
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Adicional autenticación por medio de Active Directory y enjaulamiento en la subred definida sin poder ser visto desde otras WLANs y desde clientes de la misma WLAN.

Generación de direccionamiento IP mediante uso de DHCP Server de Windows 2008 R2 ambiente de desarrollo, con provisión de direccionamiento en subred 192.168.102.0/24, se ilustra en figura 61.

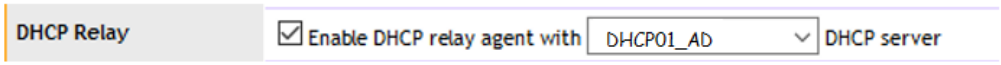

Figura 61. Configuración DHCP para RG-02
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Consta lista de accesos a destinos requeridos para uso del correo, Intranet, DNS, DHCP, proxy, antivirus, mensajería interna, control de solicitudes. (Se identifica requerir accesos a los equipos

internos del dominio de desarrollo, y equipos de producción provistos para pruebas y validaciones), se ilustra en figura 62.

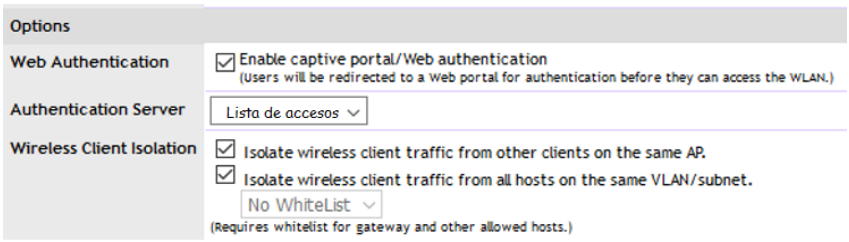

Figura 62. Autenticación Active Directory para RG-02
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Ocultar el SSID, se ilustra en figura 63.

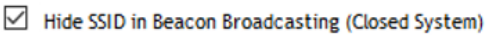

Figura 63. Ocultar SSID para RG-02
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Definir una tasa límite de uso de AB, se ilustra en figura 64.

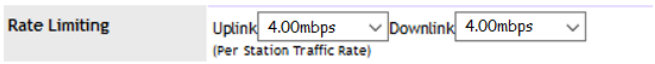

Figura 64. Tasa límite Uso de AB para RG-02
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

No solicitar a menudo el ingreso de clave, se ilustra en figura 65.

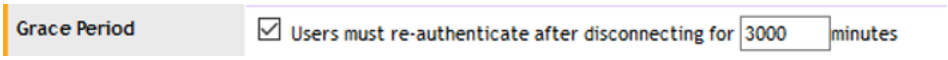

Figura 65. Tiempo para re autenticación para RG-02
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Mantener trazabilidad de toda acción del cliente, se ilustra en figura 66.

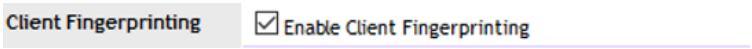

Figura 66. Obtener logs de conexión en red RG-02
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

La red debe estar disponible en horario definido, se ilustra en figura 67.

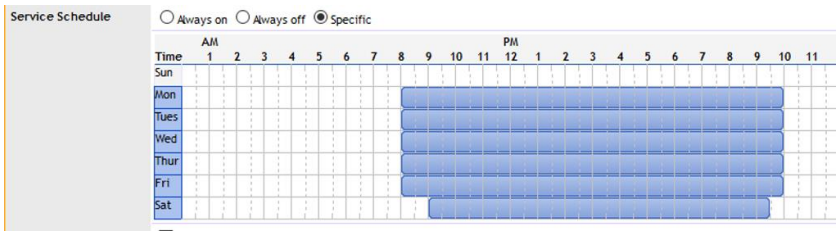

Figura 67. Horario de habilitación red RG-02
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Uso de proxy, se ilustra en figura 68.

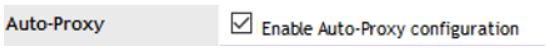

Figura 68. Uso De proxy red RG-02
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Red Clientes y Proveedores

Se coloca el nombre de la WLAN y del ESSID como **RG-03** manteniendo trazabilidad con su requerimiento funcional. Según definición se contempla proveer una experiencia de usuario de tipo guest access con provisión de clave temporal. Esta red no debe tener acceso alguno a la red interna de datos y proveer acceso de Internet con limitaciones (hacia sitios). Clave de acceso debe ser útil solo desde un equipo y se debe exponer previo a la conexión un aviso de acuerdo de servicio y aceptación de términos de uso, se ilustra en figura 69.

Tipo de uso WLAN: Guest access

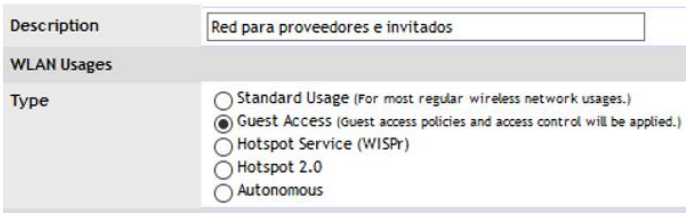

Figura 69. Tipo WLAN para RG-03
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Método de autenticación: Abierto, encripción WPA-Mixed con algoritmo de tipo Automático y frase de acceso: publico2016.Se considera aislamiento en la subred definida sin poder ser visto desde otras WLANs y desde clientes de la misma WLAN, se ilustra en figura 70.

Nota: En un inicio de las pruebas no se colocaría frase de acceso pero se verifica la posibilidad de solicitudes de acceso no previstas al no existir esta validación. Se define el colocar una frase que será cambiada periódicamente.

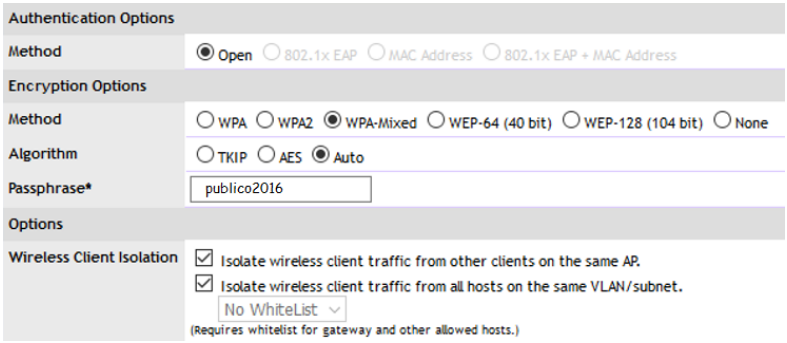

Figura 70. Autenticación y encripción para RG-03
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Definir una tasa límite de uso de AB, se ilustra en figura 71.

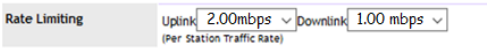

Figura 71. Tasa límite Uso de AB para RG-03
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Mantener trazabilidad de toda acción del cliente, se ilustra en figura 72.

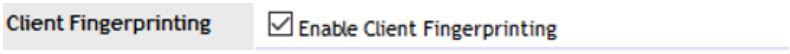

Figura 72. Obtener logs de conexión en red RG-03
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

La red debe estar disponible en horario definido, se ilustra en figura 73.

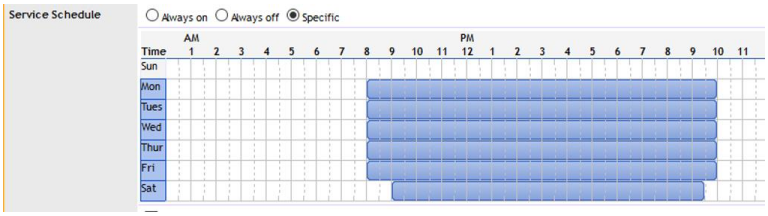

Figura 73. Horario de habilitación red RG-03
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Limitar un solo dispositivo por clave generada, se ilustra en figura 74.

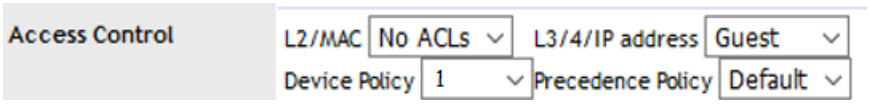

Figura 74. Número máximo de dispositivos red RG-03
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Proveer direccionamiento IP provisto por la solución. Se identifica la necesidad de crear una nueva subred que no tenga ninguna relación con la red interna, para el caso de la prueba se configura la subred 192.168.103.0/24 (se adjunta solicitud de creación de red adicional en firewall de salida Internet), se ilustra en figura 75.

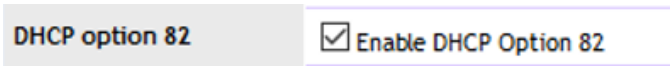

Figura 75. Configuración DHCP para RG-03
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Desconectar el equipo en caso de inactividad, se ilustra en figura 76.

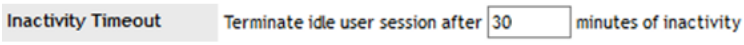

Figura 76. Definición de tiempo de inactividad para RG-03
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Términos de uso y aceptación de acceso a la red pueden ser editados según las necesidades internas, se ilustra en figura 77.

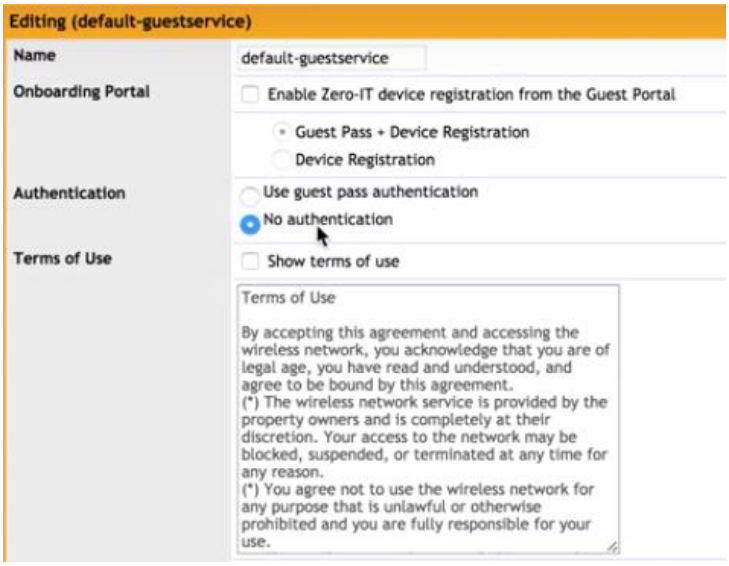

Figura 77. Configuración de Términos de uso y aceptación de acceso para RG-03
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Red Equipos celulares

Se coloca el nombre de la WLAN y del ESSID como **RG-04** manteniendo trazabilidad con su requerimiento funcional. Según definición se contempla proveer una experiencia de usuario similar a la existente en su Plan Celular y al acceso existente al conectar en un sitio externo (domicilio, punto de acceso público). Esta red no debe tener acceso alguno a la red interna de datos y proveer acceso de Internet con limitaciones (hacia sitios). Debe contemplar restricción por Mac address para evitar acceso de usuarios no permitidos.

Tipo de uso WLAN: Guest Access, se ilustra en figura 78.

Figura 78 Tipo WLAN para RG-04
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Método de autenticación: Abierto, encripción WPA-Mixed con algoritmo de tipo Automático y frase de acceso: publico2016. Se considera aislamiento en la subred definida sin poder ser visto desde otras WLANs y desde clientes de la misma WLAN, se ilustra en figura 79.

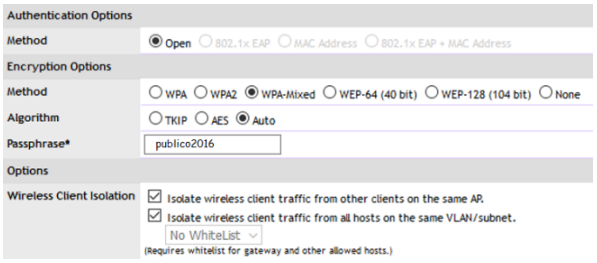

Figura 79. Autenticación y encripción para RG-04
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Definir una tasa límite de uso de AB, se ilustra en figura 80.

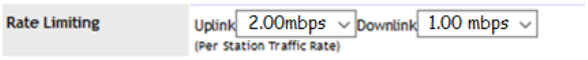

Figura 80. Tasa límite Uso de AB para RG-04
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Mantener trazabilidad de toda acción del cliente, se ilustra en figura 81.

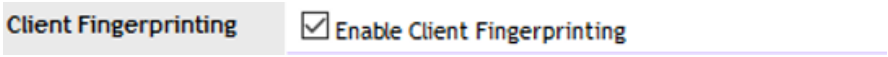

Figura 81. Obtener logs de conexión en red RG-04
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

La red debe estar disponible en horario definido, se ilustra en figura 82.

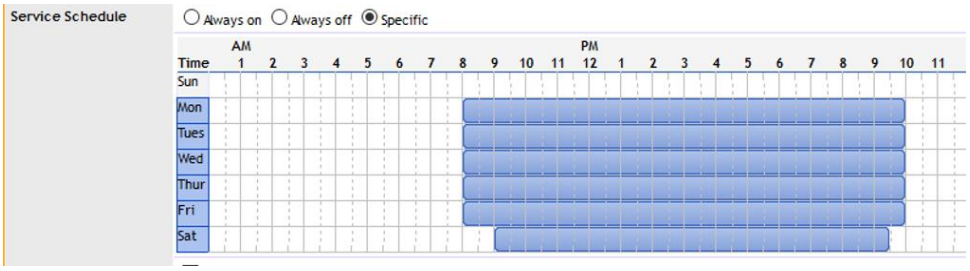

Figura 82. Horario de habilitación red RG-04
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Proveer direccionamiento IP provisto por la solución. Se usa la subred 192.168.103.0/24, se ilustra en figura 83.

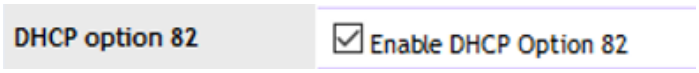

Figura 83. Configuración DHCP para RG-04
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Desconectar el equipo en caso de inactividad, se ilustra en figura 84.

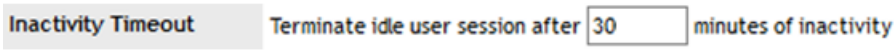

Figura 84. Definición de tiempo de inactividad para RG-04
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

No se usará autenticación guest access pero si se define acceso por registro de dispositivo, se ilustra en figura 85.

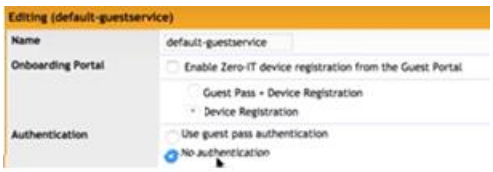

Figura 85. Registro previo de equipos RG-04
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Configuraciones estándar

Se define la capacidad máxima de usuarios concurrentes con un valor de 100 clientes, se ilustra en figura 86.

Figura 86. Máximo de clientes concurrentes
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Se define la cantidad máxima de usuarios por cada WLAN con un valor de 30 clientes, se ilustra en figura 87.

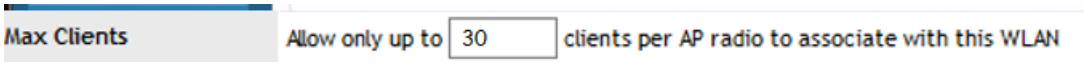

Figura 87. Máximo de clientes por AP
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Se identifica poder presentar las WLANs según necesidades en base al piso que corresponden, se permite para el caso definir grupos de WLANs mismos que pueden ser colocados por AP, se ilustra en figura 88.

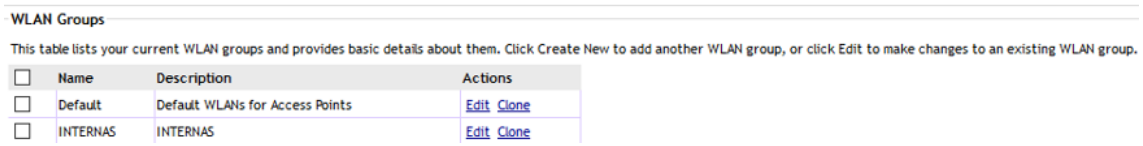

Figura 88. Grupos de WLANs
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Los APs y el equipo de Administración poseen SNMP v3. Se valida puedan ser administrados desde las herramientas de Administración existentes. Se requiere agregar equipos de monitoreo en lista de acceso 113, se adjunta formulario.

Se valida se brinde detalles de cualquier acción realizada: acoplamiento de nuevos APs, cambios en configuraciones, adhesión de un equipo a una WLAN, se ilustra en figura 89.

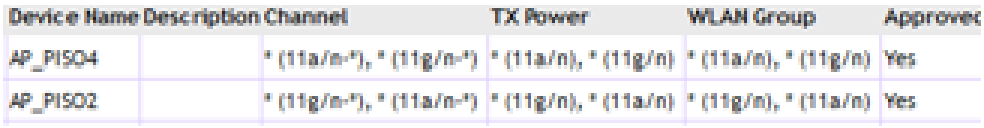

Figura 89. Detalle de APS
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Resultados (en base a lo considerado en puntos de HLD)

- Existe compatibilidad para adherir nuevos equipos en las herramienta de administración y monitoreo de la institución
- No se presenta novedad alguna respecto a acoplar puntos de red en cada piso, se evidencia verificar lugar geográfico a instalar bajo consideraciones existentes. Ambientes de desarrollo y test requerirán configurar puerto a ser colocado el AP en la VLAN correspondiente.

- Se identifica que el alcance de las WLAN abarcan cobertura parcial al piso superior e inferior al mismo
- Se requiere definir nueva subred para WLAN en ambiente producción y configuraciones en equipos internos adicionales (Active Directory, firewall, DHCP, DNS, Forefront, antivirus, listas de acceso (desarrollo y test))
- Solución a ser contemplada permite el cumplimiento de los requerimientos funcionales y no funcionales

Detalle de configuraciones críticas a tomar en cuenta

- Definir nomenclatura equipos de comunicaciones a ser implementados
- Definir clave de acceso para herramienta de administración
- Definir restricciones de acceso a la url existente por restricción ICMP y de puertos desde equipos permitidos
- Definir roles de acceso a la Consola
- Definir nombres para WLANs
- Contemplar listado de equipos de alta gerencia y medio mando (Mac address)
- Crear conexión para uso de autenticación por medio de Active Directory
- Colocar prioridad de uso de WLAN
- Contemplar tarifas de conexión
- Definir lista de accesos hacia servicios internos
- Contemplar acceso a VLAN de desarrollo y test desde equipos de comunicaciones de acceso en fase de piloto y pruebas
- Establecer horarios de uso de las WLANs

- Configurar subredes en firewall de salida a Internet
- Configurar subredes en equipo Proxy
- Configurar cambios en Active Directory en sites y políticas de acceso de usuario de Active Directory para uso o no de proxy a usuarios
- Definir subredes para la solución inalámbrica en ambiente de producción
- Establecer configuraciones para monitoreo SNMP

Fase de Diseño

Documento LLD

Aplica **restricción interna**

Introducción

El presente documento tiene como fin el especificar a detalle las configuraciones y cambios requeridos para acoplar la nueva solución en base a las definiciones recogidas en el documento HLD y en base a los resultados, consideraciones expuestas en la prueba de concepto. Se requiere especificar toda consideración a ser efectuada a nivel de detalle de interfaces por equipo de comunicaciones y configuraciones requeridas en los diferentes equipos.

Topología detallada de la red impactada

En la figura 90 se expone el detalle general de equipos de comunicaciones a ser impactados con la nueva solución con fines de clarificar los cambios a ser considerados y validar que dichos equipos cumplan con las especificaciones requeridas. El detalle de la topología detallada se ilustra en la figura 90.

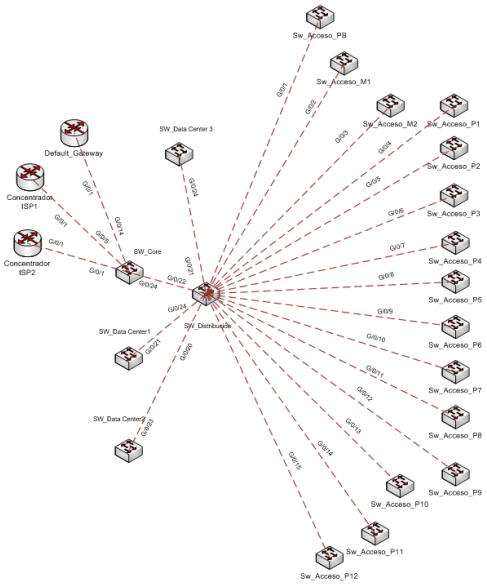

Figura 90. Topología detallada
Fuente: (Erazo, 2016), Herramienta Visio 2010, Elaboración propia

Topología detallada de la red impactada con nuevos equipos

En la figura 91 se expone detalle de nuevos equipos a ser considerados en la topología detallada y los cambios a considerarse.

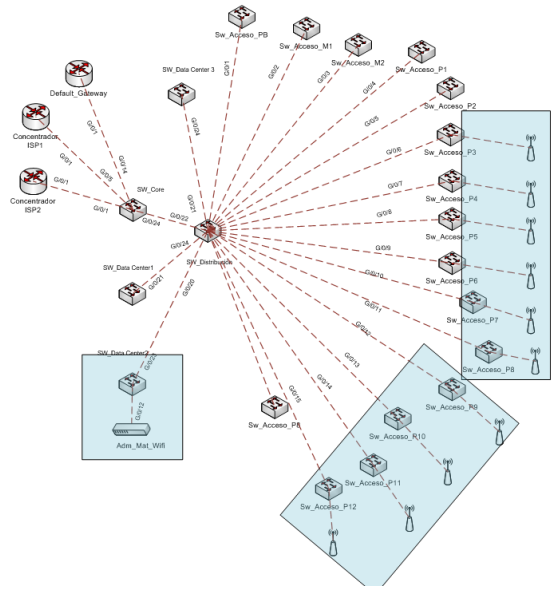

Figura 91. Topología detallada con acoplamiento de nuevos equipos
Fuente: (Erazo, 2016), Herramienta Visio 2010, Elaboración propia

Detalle de equipos

A continuación se provee detalle de direccionamiento de equipos afectados:

Switches de acceso, detalle en tabla 21

Tabla 21. Inventario switches de acceso

IP	Nombre Equipo	% Disponibilidad puertos	Total puertos	Puertos libres
10.0.207.1	SW_Acceso_PB (24) Vlan1, Vlan2	25.00%	24	6
10.0.207.4	SW_Acceso_M1 (24) Vlan1, Vlan2	29.17%	24	7
10.0.207.7	SW_Acceso_M2 (24) Vlan1, Vlan2	20.83%	24	5
10.0.207.10	SW_Acceso_P1 (24) Vlan1, Vlan2	37.50%	24	9
10.0.207.13 10.0.207.14	SW_Acceso_P2(24) SW_Acceso_P2_1(24) Vlan1, Vlan2	27.08%	48	13
10.0.207.16 10.0.207.17	SW_Acceso_P3 SW_Acceso_3_1(24) Vlan1, Vlan2	20.83%	48	10
10.0.207.19	SW_Acceso_P4 (24) Vlan1, Vlan2	37.50%	24	9
10.0.207.21	SW_Acceso_P5 (24)	33.33%	24	8
10.0.207.24	SW_Acceso_P6 (24) Vlan1, Vlan2, Vlan113, Vlan112	33.33%	24	8

10.0.207.27 10.0.207.28 10.0.207.29	SW_Acceso_P7 (24) SW_Acceso_P7 _1(24) SW_Acceso_P7 _1(24) Vlan1, Vlan2, Vlan112	27.78%	72	20
10.0.207.30 10.0.207.31	SW_Acceso_P8(24) SW_Acceso_P8_1(24) Vlan1, Vlan2, Vlan112	33.33%	48	16
10.0.207.33	SW_Acceso_P9 (24) Vlan1, Vlan2, Vlan112	33.33%	24	8
10.0.207.36	SW_Acceso_P10 (24) Vlan1, Vlan2	37.50%	24	9
10.0.207.39	SW_Acceso_P11 (24) Vlan1, Vlan2	45.83%	24	11
10.0.207.41 10.0.207.42	SW_Acceso_P12(24) Vlan1, Vlan2, Vlan 112, Vlan 113	41.67%	24	10

Fuente: (Erazo, 2016), Elaboración propia

El cambio consiste en colocar el puerto 23 de cada switch principal por piso en Vlan 112 (ambiente desarrollo), Vlan 113 (ambiente de test) y Vlan1 en ambiente de producción. Se identifica la necesidad de exponer las Vlan de desarrollo y test en los equipos de acceso de los pisos requeridos, pues al momento solo constan en los pisos 6, 7, 8, 9 y 12 (Vlan 112) y pisos 6 y 12 (Vlan113), esto según necesidad (fase del proyecto), al momento bajo necesidad de colocar los pisos 3 al 12 con acceso a Vlan 112 para el puerto 23 anteriormente especificado. Se requiere adicionalmente contemplar accesos a equipos de producción desde las Vlans de desarrollo y test.

Switches de distribución, detalle en tabla 22

Tabla 22. Inventario switches de distribución

IP	Nombre Equipo	% Disponibilidad puertos	Total puertos	Puertos libres
10.0.207.100	SW_Distribucion (48) Vlan1, Vlan2, Vlan 112, Vlan 113	33.33%	48	16
10.0.207.101	SW_Data_Center_1 (24) Vlan1	12.5%	24	3
10.0.207.102	SW_Data_Center_2 (24) Vlan1	12.5%	24	3
10.0.207.103	SW_Data_Center_3 (24) Vlan1	4.16%	24	1

Fuente: (Erazo, 2016), Elaboración propia

No requiere cambios en configuraciones ya existentes

Firewall interno, detalle en tabla 23

Tabla 23. Inventario firewall interno

IP	Nombre Equipo
10.0.200.10	Fir_Int_Mat_01

Fuente: (Erazo, 2016), Elaboración propia

Se requiere definir accesos desde subredes internas hacia equipos del core (servidores)

Firewall Externo, detalle en tabla 24

Tabla 24. Inventario firewall externo

IP	**Nombre Equipo**
10.0.201.3	Fir_Int_Mat_01
10.0.201.2	Fir_Int_Mat_02
10.0.201.1	Fir_Clu_Int_Mat

Fuente: (Erazo, 2016), Elaboración propia

Se requiere colocar salida directa a Internet desde subredes correspondientes a ambientes test y desarrollo y definir nueva subred para la red inalámbrica de producción

Router (Default Gateway), detalle en tabla 25

Tabla 25. Inventario Router central

IP	Nombre Equipo	% Disponibilidad puertos	Total puertos	Puertos libres
10.0.200.1	Ro_Default_Gateway	50%	1	2

Fuente: (Erazo, 2016), Elaboración propia

No contempla cambios pero se lo refiere ya que por el pasarán todas las peticiones de red para direccionamiento hacia la red interna y/o Internet.

Servidores, detalle en tabla 26

Tabla 26. Inventario Router central

IP	Nombre Equipo	Sistema Operativo	RAM	Dominio	Ambiente
10.0.201.10	UioMat-DC01	Windows 2008 R2	4 G	Produc.local	Productivo
10.0.201.11	UioMat-Cor01	Windows 2008 R2	8 G	Produc.local	Productivo
10.0.201.13	UioMat-Lyn01	Windows 2008 R2	6 G	Produc.local	Productivo
10.0.201.20	UioMat-Sha01	Windows 2008 R2	4 G	Produc.local	Productivo
10.0.201.28	UioMat-IIS01	Windows 2008 R2	6 G	Produc.local	Productivo
10.0.201.42	UioMat-Pro01	Windows 2008	6 G	Produc.local	Productivo

		R2			
10.0.201.60	UioMat-Ant01	Windows 2008 R2	2 G	Produc.local	Productivo
192.168.102.10	DesMat-DC01	Windows 2008 R2	2 G	Desa.local	Desarrollo
192.168.102.20	DesMat-Sha01	Windows 2008 R2	2 G	Desa.local	Desarrollo
192.168.102.28	DesMat-IIS01	Windows 2008 R2	2 G	Desa.local	Desarrollo
192.168.100.10	PruMat-DC01	Windows 2008 R2	2 G	Test.local	Testing
192.168.100.20	PruMat-Sha01	Windows 2008 R2	2 G	Test.local	Testing
192.168.100.28	PruMat-IIS01	Windows 2008 R2	2 G	Test.local	Testing

Fuente: (Erazo, 2016), Elaboración propia

Se contemplan servidores de producción impactados para los cuales se requiere accesos para la validación de la POC, consta adicionalmente equipos que se usarán desde ambientes de desarrollo y test.

Diagrama detallado de la red

En la figura 92 se expone el diagrama detallada de la red.

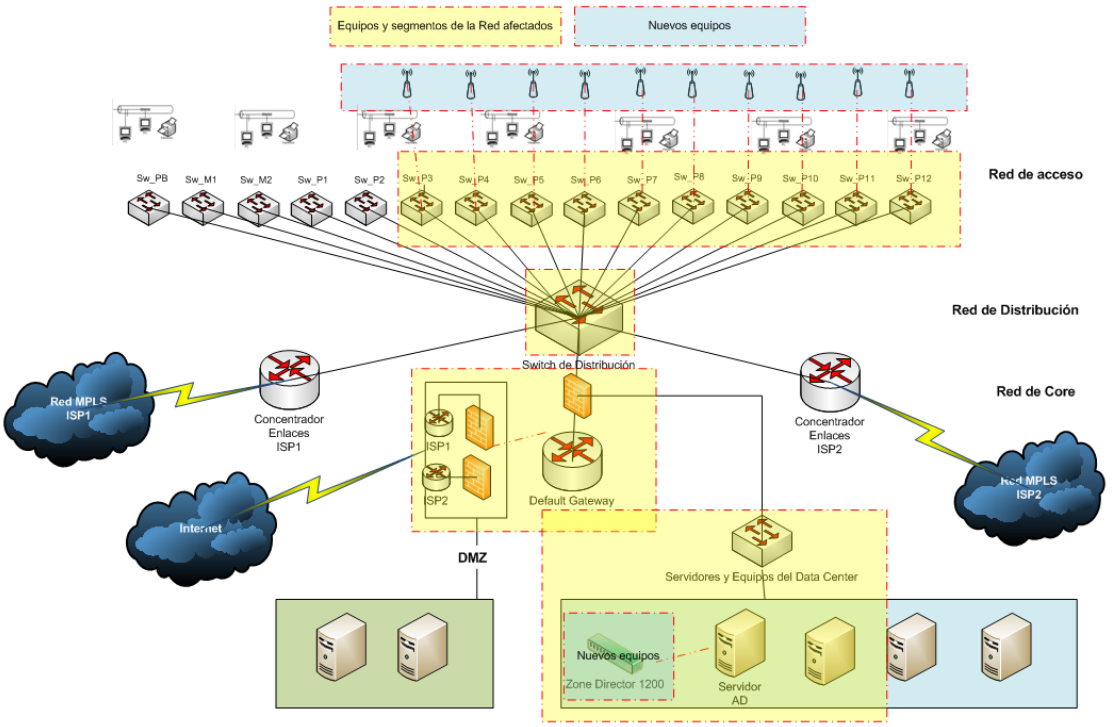

Figura 92. Diagrama detallado de red
Fuente: (Erazo, 2016), Elaboración propia

Detalle de configuraciones propuestas, uso de estándares, nomenclaturas y definiciones

Nomenclatura para nuevos equipos

Se designa la siguiente nomenclatura temporal para los equipos a ser adicionados:

- ZoneDirector01 **Consola de administración**
- AP01 **AP a colocar en Piso 7**
- AP02 **AP a colocar en Piso 8**
- AP03 **AP a colocar en Piso 9**

Nomenclatura temporal para redes WLAN, se ilustra en tabla 27

Tabla 27. Nomenclatura ESSID y descripción

Detalle de la WLAN	Ambiente desarrollo
Red alta gerencia	RG-01
Red líneas de supervisión	RG-02
Red clientes y proveedores	RG-03
Red equipos celulares	RG-04

Fuente: (Erazo, 2016), Elaboración propia

Nomenclatura Grupo WLAN

- **Todas** (Red RG-01, RG-02, RG-03, RG-04)
- **Cerradas1 (**Red RG-01, RG-02)
- **Cerradas2 (**Red RG-01, RG-02, RG-04)

Roles para Consola de Administración

Se identifica 3 roles requeridos

- Superadmin (administración total)
- Auditor (validar configuraciones de redes WLAN creadas, equipos Mac address adheridos, claves tipo guest generadas, Grupos WLAN creador, grupos WLAN a desplegar por AP, logs de conexiones, uso de CPU, memoria, con acceso lectura)
- Generador de claves guest Access, usuario con acceso para generación de accesos temporales tipo guest

Consideraciones críticas

Verificar e la Consola de administración se deshabilite la siguiente opción (por defecto habilitada), ilustrada en figura 93.

Figura 93. Política General para APs
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Configurar en la Consola de Administración la adhesión a Directorio Activo con usuario de tipo Domain Admin, se ilustra en figura 94.

Figura 94. Configuración para atar a Active Directory
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Configurar en la Consola de Administración la provisión de DHCP para las WLAN RG-01 y RG-02 y establecer autogenerada para WLANs RG03 y RG-04

DHCP por medio de servidor Windows 2008 R2 con rol DHCP, se ilustra en figura 95.

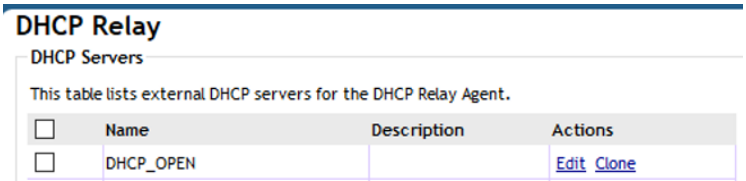

Figura 95. Configuración DHCP con servidor externo
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

DHCP auto generado por la solución

La solución provee un auto direccionamiento DHCP propio, se ilustra en la figura 96.

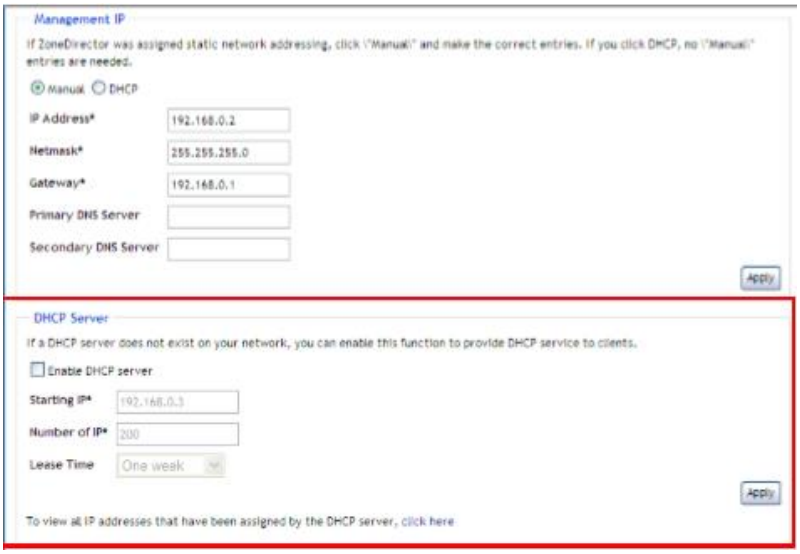

Figura 96. Configuración DHCP con servidor externo
Fuente: (Erazo, 2016), Herramienta Consola Web Zone Director (Ruckus), Elaboración propia

Configurar en proxy Forefront TMG 2013 la subred 192.168.102.0/24

Agregar subred 192.168.102.0/24 en la opción redes, se ilustra figura 97 en donde consta la opción desde donde adicionar la nueva subred establecida.

Figura 97. Agregar subred en proxy ForeFront
Fuente: (Erazo, 2016), Herramienta ForeFront 2010, Elaboración propia

Adicionar en configuración de Sites de Active Directory la subred correspondiente al ambiente configurado, en el presente caso la subred 192.168.102.0/24, se ilustra en figura 98.

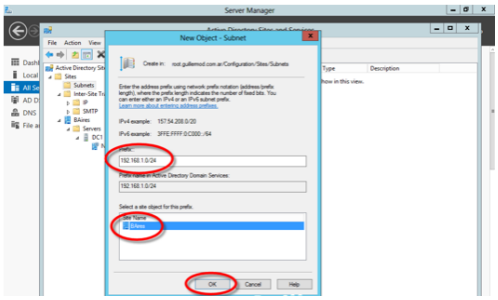

Figura 98. Agregar subred en Sites de Active Directory
Fuente: (Erazo, 2016), Herramienta Windows 2008, Elaboración propia

Agregar subred 192.168.102.0/24 dentro de objeto LAN_Fijas en firewall de salida directa a Internet, se coloca log para track de acciones efectuadas, se ilustra en figura 99.

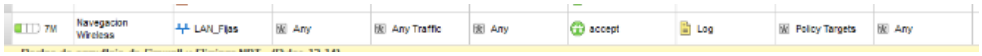

Figura 99. Agregar nuevo objeto re regla existente
Fuente: (Erazo, 2016), Herramienta firewall CheckPoint, Elaboración propia

Configurar adicionalmente QoS para brindar un valor fijo a considerar dentro de toda la capacidad de AB del canal, para el caso 5% de peso para navegación desde redes inalámbricas RG-03, RG-04, se ilustra en figura 100.

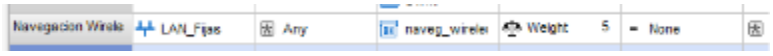

Figura 100. Configuración QoS
Fuente: (Erazo, 2016), Herramienta firewall CheckPoint, Elaboración propia

Peso de 32% del canal para navegación desde equipos de salida directa (constan dentro del grupo la subred 192.168.102.0/24),se ilustra en figura 101.

Figura 101. Configuración QoS 2
Fuente: (Erazo, 2016), Herramienta firewall CheckPoint, Elaboración propia

Permisos ICMP y SNMP

Agregar objetos de nuevos equipos en Grupo G_ICMP_Servidores, se ilustra en figura 102.

Figura 102. Configuración ICMP
Fuente: (Erazo, 2016), Herramienta firewall CheckPoint, Elaboración propia

Lo propio en Grupo G_Admin_Servidores, se ilustra en figura 103

Figura 103. Configuración ICMP 2
Fuente: (Erazo, 2016), Herramienta firewall CheckPoint, Elaboración propia

Prohibir accesos a herramientas peligrosas y emitir log de intentos generados desde equipos, se ilustra en figura 104.

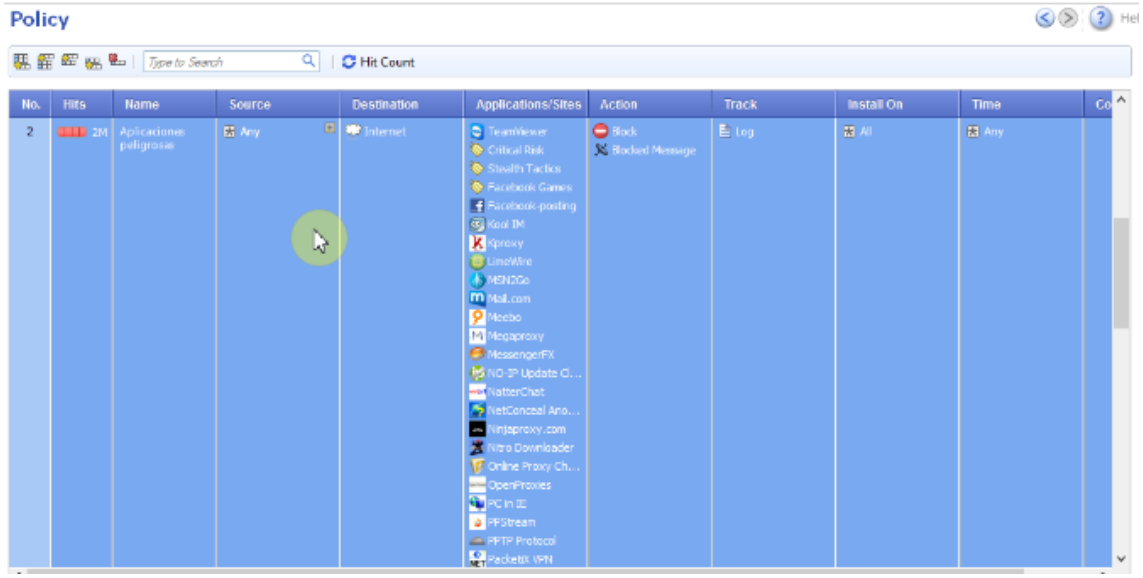

Figura 104. Aplicaciones prohibidas
Fuente: (Erazo, 2016), Herramienta firewall CheckPoint, Elaboración propia

Configurar ruta desde firewall a subred 192.168.102.0/24, se ilustra en figura 105.

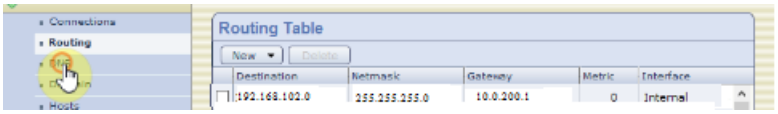

Figura 105. Aplicaciones prohibidas
Fuente: (Erazo, 2016), Herramienta firewall CheckPoint, Elaboración propia

Detalle del cableado

Se adjunta en la tabla 28 el detalle del cableado del edificio matriz.

Tabla 28. Detalle general del cableado

Nombre del edificio: edificio matriz						
Ubicación del closet de telecomunicaciones: En cada piso consta 3 metros del área del Ascensor						
Data Center: está ubicado en el Sexto Piso						
Topología lógica del cableado (árbol)						
Cableado vertical						
	Coaxial	**Fibra**	**STP**	**UTP Category 3**	**Category 5 o 6**	**Otro**
Eje vertical 1					*	
Cableado Horizontal						
	Coaxial	**Fibra**	**STP**	**UTP Category 3**	**Category 5 o 6**	**Otro**
Piso PB					*	
Piso M1					*	
Piso M2					*	
Piso P1					*	
Piso P2					*	
Piso P3					*	
Piso P4					*	
Piso P5					*	
Piso P6					*	
Piso P7					*	
Piso P8					*	
Piso P9					*	
Piso P10					*	
Piso P11					*	
Piso P12					*	
Cableado del área de trabajo						
	Coaxial	**Fibra**	**STP**	**UTP Category 3**	**Category 5 o 6**	**Otro**
Piso PB					*	
Piso M1					*	
Piso M2					*	
Piso 1					*	
Piso 2					*	
Piso 3					*	
Piso P4					*	
Piso P5					*	

Piso P6	*
Piso P7	*
Piso P8	*
Piso P9	*
Piso P10	*
Piso P11	*
Piso P12	*

Fuente: (Erazo, 2016), Elaboración propia

En base a la distribución de pisos y ante la restricción de colocar redes inalámbricas cerca de área de libre acceso se define las siguientes consideraciones, expuestas en tabla 29:

Tabla 29. Detalle general del cableado

Piso	**Grupo WLAN**
Piso 3	Cerradas1
Piso P4	Todas
Piso P5	Todas
Piso P6	Todas
Piso P7	Todas
Piso P8	Todas
Piso P9	Todas
Piso P10	Todas
Piso P11	Cerradas2
Piso P12	Cerradas2

Detalle de direccionamiento configuraciones nuevos equipos

Se define el siguiente direccionamiento para los nuevos equipos:

192.168.102.100 Adm_Mat_Wifi

192.168.102.101 Adm_Mat_AP01

192.168.102.102 Adm_Mat_AP02

192.168.102.103 Adm_Mat_AP03

Detalle de estrategias de seguridad

Se contempla el uso del estándar 802.11 ac mismo que forma parte de la solución de los APs. En cuanto a las WLAN se usará los siguientes filtrados para autenticación, visibilidad, encripción, filtrado de contenido, siendo los siguientes:

Red RG-01

Método de Autenticación por medio de filtrado **Mac address**

Servidor de Autenticación: **Active Directory**

Algoritmo: **Automático**

Método de encripción **WPA-Mixta**

Uso de frase de paso: **Si**

Estado de ESSID: **oculto**

Filtrado de contenidos: **por medio de firewall**

Red RG-02

Método de Autenticación por medio de filtrado **Mac address**

Servidor de Autenticación: **Active Directory**

Algoritmo: **Automático**

Método de encripción **WPA-Mixta**

Uso de frase de paso: **Si**

Estado de ESSID: **oculto**

Filtrado de contenidos: **por medio de proxy**

Red RG-03

Método de Autenticación **Abierta**

Servidor de Autenticación: **guest access**

Algoritmo: **Automático**

Método de encripción **WPA-Mixta**

Uso de frase de paso: **Si**

Estado de ESSID: **visible**

Filtrado de contenidos: **por medio de firewall**

Red RG-04

Método de Autenticación **Abierta**

Servidor de Autenticación: **guest Access (filtrado Mac address)**

Algoritmo: **Automático**

Método de encripción **WPA-Mixta**

Uso de frase de paso: **Si**

Estado de ESSID: **visible**

Filtrado de contenidos: **por medio de firewall**

Realizar prueba de verificación del diseño

Se re valida que toda consideración expuesta en los documentos HLD, LLD sea cumplida. La prueba de validación se ejecuta con el uso de la Consola de administración y 3 APs.

Definir estrategia final de Administración de red

Los equipos de la solución cuentan con soporte SNMP en sus tres versiones. Se valida capacidad de acoplamiento con herramientas internas de monitoreo.

Ubicación geográfica de AP

En base a consideraciones de los pisos en donde se cuenta con los pilares propios de la edificación y separaciones efectuadas con gypsum, adicional de tener las salas de reuniones en lugares estándar por piso, se vuelve mucho más práctico el definir los lugares geográficos donde se requiere colocar los APs, esto bajo la consideración de proveer excelente cobertura en áreas correspondientes a salas de reuniones y oficinas de Altos ejecutivos y líneas de supervisión. A continuación el detalle de los 3 pisos donde se ejecutará la prueba:

Piso 7, se detalla plano mediante figura 105.

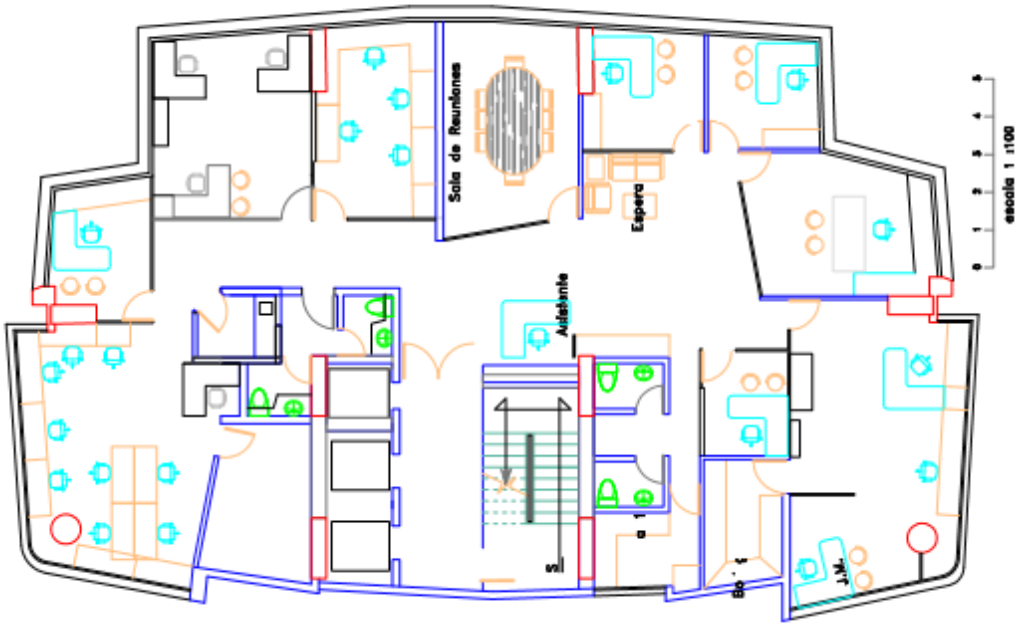

Figura 105. Plano Piso 7
Fuente: (Orozco, 2011), Herramienta AutoCAD

Piso 8, se detalla plano mediante figura 106.

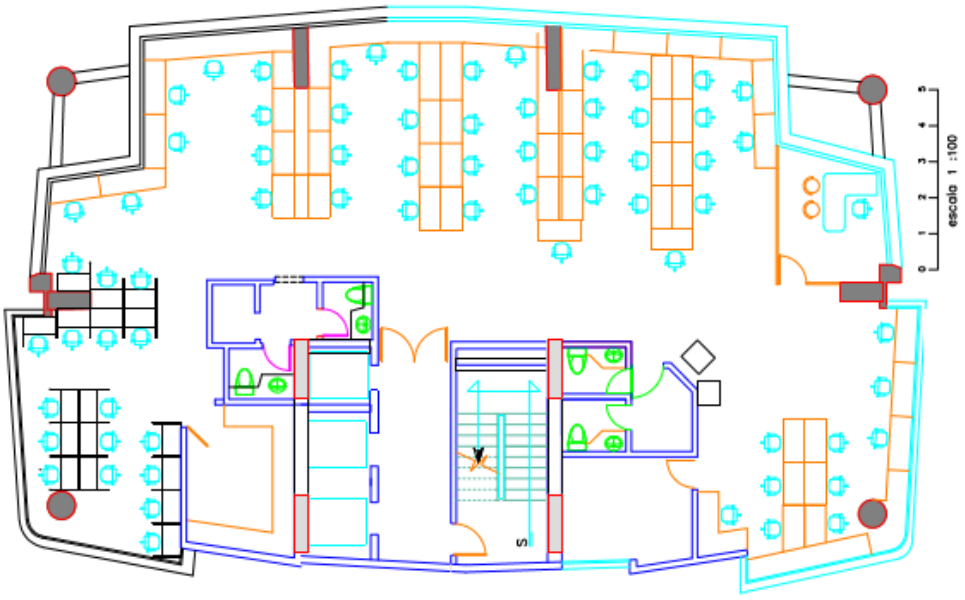

Figura 106. Plano Piso 8
Fuente: (Orozco, 2011), Herramienta AutoCAD

Piso 9, se detalla plano mediante figura 107.

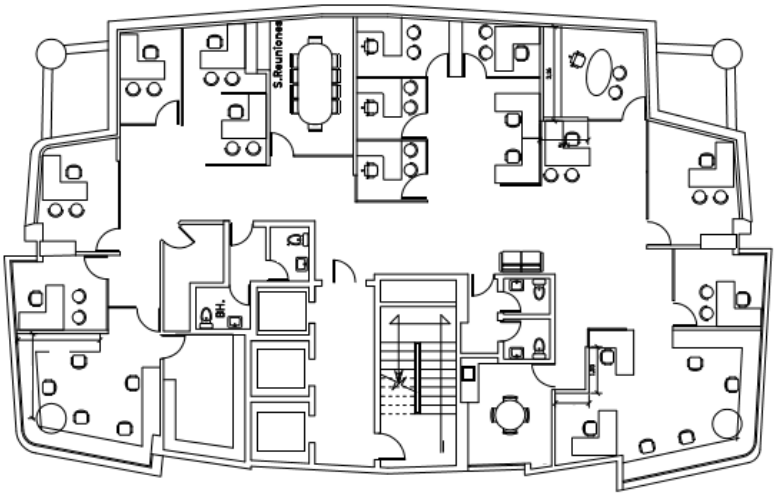

Figura 107. Plano Piso 9
Fuente: (Orozco, 2011), Herramienta AutoCAD

Con las validaciones efectuadas se verifica tener conectividad de un AP con cobertura excelente dentro del área a continuación demarcada adicional de brindar conectividad con cobertura intermedia en el piso superior e inferior, el detalle obtenido es el siguiente:

Piso 8, se detalla área de cobertura mediante figura 108.

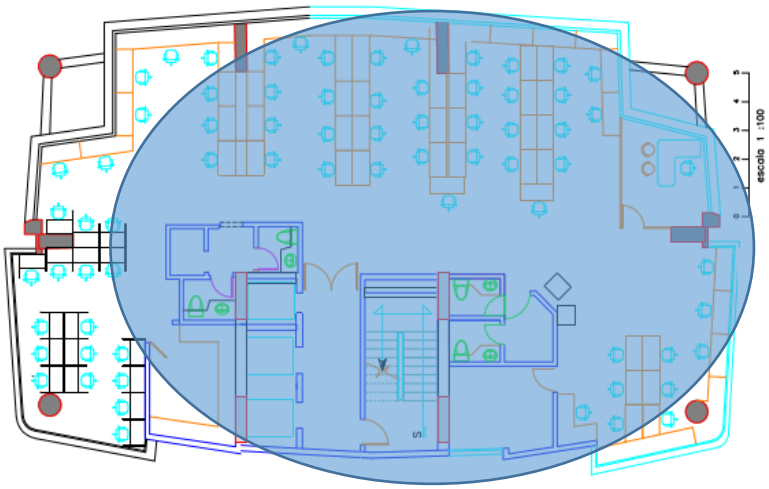

Figura 108. Plano Piso 8
Fuente: (Orozco, 2011), Herramienta AutoCAD

Piso 7, se detalla área de cobertura mediante figura 109.

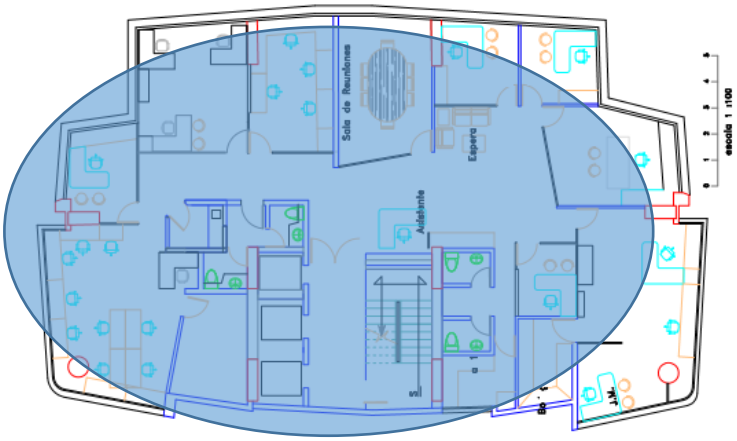

Figura 109. Plano Piso 7
Fuente: (Orozco, 2011), Herramienta AutoCAD

Piso 9, se detalla plano mediante figura 107.

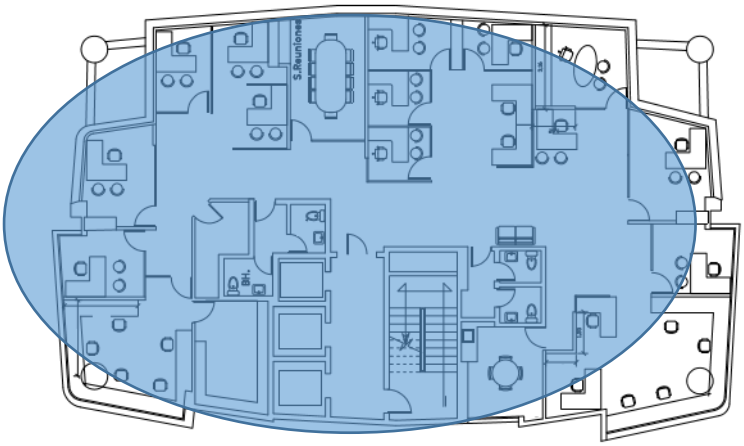

Figura 110. Plano Piso 9
Fuente: (Orozco, 2011), Herramienta AutoCAD

Siendo las consideraciones de tiempo y presupuesto limitadas, se verifica con equipos finales (Smartphone, laptop, IPad) el status de la recepción de señal del dispositivo, adicional de verificar por medio y en función de los resultados se identifica la mejor opción para colocar los

APs la siguiente, misma que provee el 99% de cobertura por cada piso. Se identifica requerir el colocar auto configuración de canales para evitar interferencias.

Piso 7, se detalla ubicación del AP mediante figura 111.

Figura 111. Plano Piso 7
Fuente: (Orozco, 2011), Herramienta AutoCAD

Piso 8, se detalla ubicación del AP mediante figura 112.

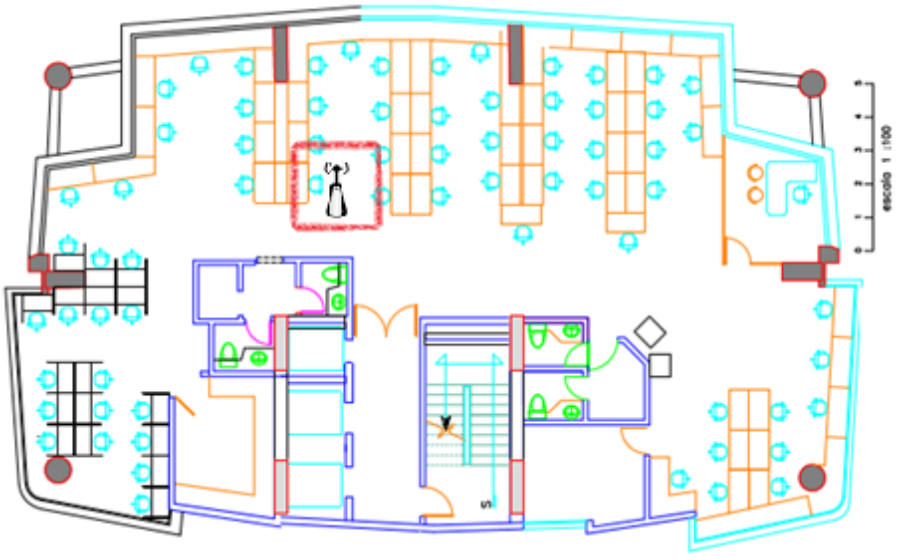

Figura 112. Plano Piso 8
Fuente: (Orozco, 2011), Herramienta AutoCAD

Piso 9, se detalla ubicación del AP mediante figura 113.

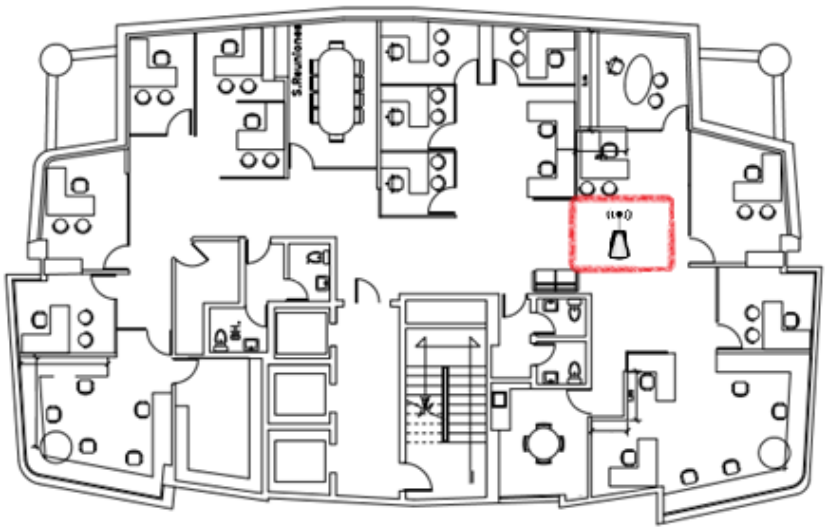

Figura 113. Plano Piso 8
Fuente: (Orozco, 2011), Herramienta AutoCAD

Bajo este lineamiento se solicita la creación de un punto de red en cada piso en el lugar expuesto. Los lugares seleccionados están lejanos a luminario, otros cableados (eléctricos, de datos).

SOW

Proyecto_Red_Inalambrica_Edf.Matriz

Octubre 2016

Versión 1.0

*(Documento requiere firmas de los stakeholders)

Aplica restricción interna

Introducción

La institución ha aprobado recientemente el proyecto de red inalámbrica en su edificio matriz en apoyo de su plan estratégico para brindar nuevos servicios al cliente interno y externo y reducir costos en lo que respecta a planes celulares provistos a los colaboradores. Además de solventar la problemática existente en demora en respuesta de aprobaciones de solicitudes por parte de las líneas de supervisión al estar imposibilitados de acceder la inexistencia de puntos de datos disponibles en las salas de reuniones y ante la inexistencia de contar con soluciones de movilidad desde sus equipos portátiles. El presente proyecto se centra en la construcción y despliegue de una solución que permita solventar el tema de movilidad y provisión de servicios inalámbricos.

Objetivos

Objetivos organizacionales

- Brindar servicios de vanguardia
- Reducir costos
- Adicionar nuevas funcionalidades al cliente interno y externo

Restricciones organizacionales

- Presupuesto limitado a 20000 USD
- Cumplir políticas internas de acceso y seguridad de la información
- Cumplir con la entrega del pedido original hasta el 11 de Noviembre 2016 (incluye cierre del proyecto)
- Acatar las regulaciones existentes acerca de inhibidores en lugares de atención al público
- Cumplir normativas existentes internas y de organismos de control

Objetivos técnicos

- Modernizar tecnologías obsoletas
- Proveer escalabilidad en la red

Restricciones técnicas

- Cumplir políticas internas de seguridad

Alcance de la solución

El alcance de la solución provista incluye el análisis y diseño de la solución inalámbrica que ha de acoplarse a la red existente brindando escalabilidad. Incluye adicionalmente toda planificación, ejecución, pruebas e implementación de la solución propuesta. Estas actividades serán ejecutadas a la interna de la institución, si bien involucra un proveedor su rol específico es en la provisión de equipos, gestión de licenciamiento y apoyo ante posible requerimiento de garantía de equipos, adicional de proveer acceso al portal propio del Vendedor para acceso a documentación delas soluciones, gestión de actualizaciones, soporte ante incidentes específicos de la solución, siendo responsabilidad del proveedor el velar por el cumplimiento de estos temas, cabe considerar es esencial el cumplimiento del proveedor en la entrega de equipos en la fecha expuesta. Por parte del área de tecnología se velará el cumplimiento de toda actividad que permita la consecución del nuevo servicio de movilidad, incluye capacitación a personal interno que proveerá accesos tipo guest y colaboradores que auditarán y efectuarán monitoreo desde la solución. Forma parte del proyecto la provisión de puntos datos requeridos para los APs así como equipos de comunicaciones requeridos (switches de acceso).

Las entregas específicas y los hitos relevantes se enumeran en la sección Requisitos de trabajo, Fechas de entrega e hitos que constan en el presente documento.

No forma parte del actual proyecto provisión de nuevos enlaces, valga aclarar se reutiliza el enlace existe que provee salida a Internet a toda la institución, no incluye cambio alguno sobre la aplicación interna de control de solicitudes.

Período de ejecución

Se contempla ejecutar toda actividad del proyecto en el lapso (40 días) a partir del 3 de Octubre 2016 y hasta el 11 de Noviembre 2016. Toda actividad requerida debe ser planificada y ejecutada dentro de este plazo. De contemplarse cambios de alcance o cualquier modificación deberá ser tratada por todo stakeholder para su revisión y discusión y deberá ser formalizado por medio de una solicitud de control de cambio.

Lugar de ejecución

Toda actividad será ejecutada dentro de las instalaciones del edificio matriz y deberá usarse una red de ambiente no productivo garantizando no impactar actividad alguna en ambiente producción, incluso y de ocurrir deberá reversarse inmediatamente la implementación efectuada mediante rollback en base a lo estipulado en los documentos correspondientes.

Se acuerda con el proveedor de la solución inalámbrica el mantener una reunión semanal a efectuarse una vez por semana (día viernes a las 17:00) para mantener una reunión de status semanal.

Requisitos de trabajo

Se detalla tareas más importantes y entregables a ser provistos en cada una de las fases que forman parte del proyecto. Cabe considerar se basa en detalle de ETVX de metodología interna.

Fase Inicio

Documento de necesidades

Acta de constitución del Proyecto

Reunión de kick-off

Documento CRD

Documento estrategia Arquitectura de red

Documento caso de negocio

Gantt inicial Alto nivel

Fase Análisis

Documento Estado de salud de la red

Documento HLD

Documento resultados POC

Gantt detallado

Fase Diseño

Documento LLD

SOW

Gantt final

Fase Prototipo

Documento Plan de implementación y roll back hacia ambiente de test

Documento pruebas de funcionalidad, pruebas negativas, de rendimiento

Fase Pruebas

Documento resultados de pruebas

Documento Plan de implementación y roll back hacia ambiente de producción

Fase Implementación

Informe de resultados

Fase Post implementación

Documento Acta de aceptación final TI

Fase monitoreo y control

Documento definiciones de monitoreo

Fase Cierre

Acta formal de cierre

Detalle de requerimientos funcionales, expuesto en tabla 30.

Tabla 30. Detalle requerimientos funcionales

Servicio requerido	Criterios de aceptación	Nivel de aceptación	Método de seguimiento
Crear una red inalámbrica de acceso para la alta gerencia. Deberá contemplar una experiencia de usuario similar a la existente cuando posee conexión LAN, es decir con acceso a la red interna, acceso a Internet sin uso de proxy, acceso a impresoras, Portal interno, correo, FTP, mensajería, aplicativos de uso interno, acceso a cámaras de video vigilancia. Al tener accesos sin restricción debe contar con autenticación por filtrado de	Documentación Cumplimiento de la solicitud	100% funcional Cumplimiento del despliegue a producción hasta el 6 de Noviembre 2016	Muestreo aleatorio

dirección MAC (podrá registrarse equipos adicionales: celulares, tablets), control de acceso por medio de Active Directory. Estos accesos deben ser controlados por el oficial de seguridades.			
Crear una red inalámbrica de acceso para uso de primeras y segundas líneas de supervisión y usuarios con laptop. Deberá contemplar una experiencia de usuario similar a la existente cuando posee conexión LAN, es decir con acceso (limitado) a la red interna, acceso a Internet mediante uso de proxy, acceso al Portal interno, correo, mensajería, aplicativos de uso interno. Al tener accesos a la red interna debe contar con autenticación por filtrado de dirección MAC (listado provisto por área de tecnología de todo equipo portátil suministrado a usuarios de matriz para los usuarios establecidos), control de acceso por medio de Active Directory. Estos accesos deben ser controlados por el	Documentación Cumplimiento de la solicitud	100% funcional Cumplimiento del despliegue a producción hasta el 6 de Noviembre 2016	Muestreo aleatorio

Responsable de tecnología y bajo monitoreo y auditoria del oficial de seguridades.			
Crear una red inalámbrica de acceso para uso de clientes y proveedores. Deberá contemplar una experiencia de usuario similar de tipo guest Access con provisión de acceso mediante clave temporal. Esta red es de uso exclusivo para acceso a Internet sin acceso alguno a la red de datos. Además deberá restringirse el uso de redes sociales, gestores de descarga, acceso remoto, contenido multimedia (YouTube, emisión de radio), acceso muy limitado. La clave de acceso provista deberá ser útil únicamente con un equipo y deberá tener periodicidad. Deberá suministrarse un aviso de acuerdo de servicio previo a conectarse a la red, en donde se exponga que el equipo estará siendo monitoreado.	Documentación Cumplimiento de la solicitud	100% funcional Cumplimiento del despliegue a producción hasta el 6 de Noviembre 2016	Muestreo aleatorio
Crear una red inalámbrica para uso de equipos celulares de	Documentación	100% funcional	Muestreo aleatorio

colaboradores que poseen Plan institucional que permita obtener funcionalidad similar a la existente cuando están registrados con su Plan de Internet celular. Se proveerá una clave general para acceso a esta red y será adicionalmente registrada mediante acceso por Mac address (para evitar difusión a usuarios no permitidos)	Cumplimiento de la solicitud	Cumplimiento del despliegue a producción hasta el 6 de Noviembre 2016	
Proveer una solución adaptativa que permita crear nuevas redes inalámbricas sin impactar las ya existentes	Documentación	100% conformidad	Evidencia de prueba ejecutada
Las redes inalámbricas para acceso a usuarios finales no debe tener acceso a la red interna de la institución	Documentación	100% cumplimiento	Evidencia de prueba ejecutada
Los accesos por medio de uso de Active Directory deben	Documentación	100% cumplimiento	Evidencia de prueba

dejar pistas en el sistema a ser implementado a fin de validar que concuerde el acceso del usuario y equipo			ejecutada
Las redes no deben ser desplegadas en área de acceso Público, mucho menos donde se brinde servicios de atención de cajas (ingreso/retiro de dineros)	Documentación	100% cumplimiento	Muestreo aleatorio
Todo equipo de la solución debe ser incluido en las herramientas de monitoreo de la institución	Documentación	100% cumplimiento	Muestreo aleatorio
Todo cambio efectuado en las configuraciones debe ser reportado al administrador del centro de cómputo, área de redes, oficial de seguridades, oficial de riesgos	Documentación	100% cumplimiento	Muestreo aleatorio

Fuente: (Erazo, 2016), Elaboración propia

Detalle de requerimientos no funcionales, descrito en tabla 31

Tabla 31. Detalle requerimientos no funcionales

NFR-001	Las redes inalámbricas deben brindar acceso a 200 usuarios concurrentes y al menos 20 usuarios por AP y permitir escalabilidad para futuro uso o despliegue
NFR-002	Las redes inalámbricas deben estar disponibles durante horarios laborables únicamente
NFR-003	Los APs deben proveer servicio con lata cobertura en áreas donde constan salas de reuniones de los diferentes pisos y oficinas de alta gerencia

Fuente: (Erazo, 2016), Elaboración propia

Fechas de entrega e hitos

A continuación un detalle de los compromisos de entrega e hitos identificados para el presente proyecto:

Inicio del proyecto	3 de Octubre 2016
Entrega de necesidades	3 de Octubre 2016
Efectuar Acta de constitución del proyecto	4 de Octubre 2016
Envío de propuestas	7 de Octubre 2016
Selección de proveedor	11 de Octubre 2016
Efectuar prototipo	13 de Octubre 2016
Resultados de Pruebas	17 de Octubre 2016
Compra de equipos	21 de Octubre 2016

Ejecución de pruebas finales	25 de Octubre 2016
Capacitación a usuarios	26 de Octubre 2016
Despliegue en producción	28 de Octubre 2016
Acta de cierre	9 de Noviembre 2016
Cierre del proyecto	11 de Noviembre 2016

Criterios de aceptación

La aceptación de todos los entregables definidos en las diferentes fases, deben ser aprobados por el Sponsor del proyecto Dr. Juan Yépez adicional de los Señores: Ing. Daniel Rosero (oficial de seguridades), previo aval de verificación a realizarse por parte del Señor Ing. Luis López (Sub gerente de tecnología) al ejecutor del proyecto el Señor Ing. Juan Pablo Moreno. Es mandatorio el obtener el OK de aceptación y cumplimiento del CheckList de cada fase del proyecto para poder avanzar a una fase siguiente (solo en fase Prototipo podrá paralelizarse las actividades correspondientes junto con las de fase Análisis/Diseño). Una vez que se cuente con el cumplimiento de todas las fases y de obtener los OKs de aceptación de cumplimiento de la fase anterior podrá procederse con el cierre del proyecto. El no cumplimiento o desacuerdo con alguna actividad del proyecto repercutirá directamente en la calificación de objetivos del área de tecnología y en la encuesta de satisfacción final.

Otros requisitos

- Debe contemplarse accesos hacia las diferentes WLANs para todo miembro del proyecto y deberá regularizarse todo pedido de configuraciones en equipos existente mediante los formularios del caso.
- Deberá mantenerse respaldos periódicos de las configuraciones de los equipos

Costo del proyecto

Se contempla un presupuesto de 20000 USD para el presente proyecto, mismo que contempla rubros requeridos para compra de nuevos equipos, licenciamiento, soporte a 3 años de solución a implementar, provisión de equipos requeridos en red existente así como instalación de puntos de datos requeridos para los nuevos equipos.

Detalle de costos, detalle en tabla 32

Tabla 32. Detalle costos

Cantidad	Detalle	Costo	IVA	Total
1	Ruckus Zone Director 1200	2265,00	317.10	$ 2582.10
15	ZoneFlex R710	9750,00	1365	$ 11115
1	Licenciamiento, soporte (3 años)	1950	273	$ 2223
10	Punto de datos	1300	182	$ 1482
2	Switch HP 24 Puertos (1910)	1000	114	$1114

Fuente: (Erazo, 2016), Elaboración propia

Total: $ 18542.10

Los equipos poseen cumplimiento de entrega de 1 día a contar desde el envío formal y aceptación de la propuesta del proveedor. La realización de los puntos de red presenta cumplimiento de 3 días laborables una vez aprobada la propuesta.

Supuestos

- Existencia de inventario de equipos, IPs, puertos, diseño de red actualizado
- Contar con configuración de tarjeta inalámbrica de equipos finales de usuarios
- Contar con punto de datos para los APs a ser colocados en cada piso
- Enlaces de acceso a Internet ya existentes, solución no contempla costos de provisión de nuevos enlaces

Restricciones

- Presupuesto no puede superar los 20000 USD y debe estar listo en 40 días
- Actividades deben ser ejecutadas durante la jornada laborable, no está autorizado el uso de horas extras
- Debe contemplarse restricciones de acuerdo a lo establecido para cada red, en base a las definiciones acordadas
- No deberá exponerse acceso a la red inalámbrica desde ubicaciones de acceso público de clientes (cajas, balcón de servicio, área de crédito)

Riesgos

- No poder cumplir la fecha de acuerdo establecido por limitaciones de costo y esfuerzo
- No poder proveer una solución tecnológica robusta al existir limitaciones de costo y esfuerzo, teniendo impacto directo en la calidad del entregable

Acuerdos de servicio

Se contempla que el servicio de red wireless a ser provisto no es catalogado como un servicio crítico de la institución (en su primera etapa); esto debido a no existir el presupuesto del caso para proveer contingencia. Si bien no será considerado dentro del documento de SLA existente se considera la necesidad de mantener un monitoreo permanente de los equipos, contemplar equipos de backup ante posibles fallos (APs).

Aprobación

Contemplar firmas de todo stakeholder

Creación Prototipo

Documento LLD actualizado

Por medio del presente documento se acopla actualizaciones al documento LLD para contemplar la integración de la solución completa en ambiente de desarrollo. Se considera solo los cambios a ser requeridos para este fin.

Detalle de equipos (cambios a ser requeridos)

A continuación se provee detalle de direccionamiento de equipos afectados:

Switches de acceso, descrito en tabla 33

Tabla 33. Detalle switches de acceso

IP	Nombre Equipo	% Disponibilidad puertos	Total puertos	Puertos libres	Cambios requeridos

10.0.207.1	SW_Acceso_PB (24) Vlan1, Vlan2	25.00%	24	6	No aplica
10.0.207.4	SW_Acceso_M1 (24) Vlan1, Vlan2	29.17%	24	7	No aplica
10.0.207.7	SW_Acceso_M2 (24) Vlan1, Vlan2	20.83%	24	5	No aplica
10.0.207.10	SW_Acceso_P1 (24) Vlan1, Vlan2	37.50%	24	9	No aplica
10.0.207.13 10.0.207.14	SW_Acceso_P2(24) SW_Acceso_P2_1(24) Vlan1, Vlan2	27.08%	48	13	No aplica
10.0.207.16 10.0.207.17	SW_Acceso_P3 SW_Acceso_3_1(24) Vlan1, Vlan2	20.83%	48	10	Habilitar VLan112, colocar puerto 23 de cada switch principal en dicha Vlan
10.0.207.19	SW_Acceso_P4 (24) Vlan1, Vlan2	37.50%	24	9	Habilitar VLan112, colocar puerto 23 de cada switch principal en dicha Vlan
10.0.207.21	SW_Acceso_P5 (24)	33.33%	24	8	Habilitar VLan112, colocar puerto 23 de cada switch principal en dicha Vlan
10.0.207.24	SW_Acceso_P6 (24)	33.33%	24	8	Habilitar VLan112,

	Vlan1, Vlan2, Vlan113, Vlan112				colocar puerto 23 de cada switch principal en dicha Vlan
10.0.207.27 10.0.207.28 10.0.207.29	SW_Acceso_P7 (24) SW_Acceso_P7 _1(24) SW_Acceso_P7 _1(24) Vlan1, Vlan2, Vlan112	27.78%	72	20	Habilitar VLan112, colocar puerto 23 de cada switch principal en dicha Vlan
10.0.207.30 10.0.207.31	SW_Acceso_P8(24) SW_Acceso_P8_1(24) Vlan1, Vlan2, Vlan112	33.33%	48	16	Habilitar VLan112, colocar puerto 23 de cada switch principal en dicha Vlan
10.0.207.33	SW_Acceso_P9 (24) Vlan1, Vlan2, Vlan112	33.33%	24	8	Habilitar VLan112, colocar puerto 23 de cada switch principal en dicha Vlan
10.0.207.36	SW_Acceso_P10 (24) Vlan1, Vlan2	37.50%	24	9	Habilitar VLan112, colocar puerto 23 de cada switch principal en dicha Vlan
10.0.207.39	SW_Acceso_P11 (24)	45.83%	24	11	Habilitar VLan112,

	Vlan1, Vlan2				colocar puerto 23 de cada switch principal en dicha Vlan
10.0.207.41 10.0.207.42	SW_Acceso_P12(24) Vlan1, Vlan2, Vlan 112, Vlan 113	41.67%	24	10	Habilitar VLan112, colocar puerto 23 de cada switch principal en dicha Vlan

Fuente: (Erazo, 2016), Elaboración propia

Switches de distribución, descrito en tabla 34

Tabla 34. Detalle switches de distribución

IP	Nombre Equipo	% Disponibilidad puertos	Total puertos	Puertos libres	Cambios requeridos
10.0.207.100	SW_Distribucion (48) Vlan1, Vlan2, Vlan 112, Vlan 113	33.33%	48	16	No aplica

Fuente: (Erazo, 2016), Elaboración propia

Nomenclatura y direccionamiento para nuevos equipos

Se designa la siguiente nomenclatura (definitiva) para los equipos a ser adicionados:

- Adm_Mat_Wifi 192.168.102.100 **Consola de administración**
- Adm_Mat_AP01 192.168.102.101 **AP a colocar en Piso 3**
- Adm_Mat_AP02 192.168.102.102 **AP a colocar en Piso 4**
- Adm_Mat_AP03 192.168.102.103 **AP a colocar en Piso 5**

- Adm_Mat_AP04 192.168.102.104 **AP a colocar en Piso 6**
- Adm_Mat_AP05 192.168.102.105 **AP a colocar en Piso 7**
- Adm_Mat_AP06 192.168.102.106 **AP a colocar en Piso 8**
- Adm_Mat_AP07 192.168.102.107 **AP a colocar en Piso 9**
- Adm_Mat_AP08 192.168.102.108 **AP a colocar en Piso 10**
- Adm_Mat_AP09 192.168.102.109 **AP a colocar en Piso 11**
- Adm_Mat_AP10 192.168.102.110 **AP a colocar en Piso 12**

Documento de pruebas de funcionalidad, pruebas negativas, pruebas de rendimiento

Pruebas detalladas para red de alta gerencia

- Validar que el nombre de la WLAN pueda ser cambiada (RG-01) por RG-10 y validar se mantengan las configuraciones establecidas en la Consola según lineamientos definidos
- Validar ingreso de equipo con Mac address registrada (en la Consola)
- Validar ingreso de equipo con Mac address no registrada (en la Consola)
- Validar ingreso de pre frase correcta, validar logs, status
- Validar ingreso de pre frase incorrecta, validar logs, status
- Validar direccionamiento provisto por medio de DHCP de Servidor Windows 2008, verificar en DHCP de Windows
- Validar ingreso de credenciales de Active Directory y aplicación de políticas de usuario con usuario y clave correcta
- Validar ingreso de credenciales de Active Directory y aplicación de políticas de usuario con usuario y/o clave incorrecta
- Validar desde varios dispositivos que el SSID no pueda ser visualizado

- Validar con usuario y clave correcta y una vez logueado el usuario de Active Directory no solicite el ingreso de clave al menos por dos horas
- Verificar en la Consola de administración exista rastros del equipo adicionado a la WLAN
- Verificar que la red WLAN este solo disponible entre las 08:00 a 22:00
- Verificar el AB disponible para la red (4 Mbps Subida y 4 Mbps de bajada)
- Acceder a la WLAN con 5 diferentes usuarios y efectuar peticiones hacia varios tipos de contenidos, verificar se ejecute balanceo de carga entre los usuarios
- Validar conectividad hacia equipos de la red interna (experiencia de usuario similar a la existente al estar conecta de forma alámbrica)
- Verificar no exista conectividad hacia otras WLANs
- Verificar no exista conectividad y vista de otros clientes de las misma WLAN
- Validar restricción de acceso a sitios prohibidos (PSP, Pornografía, Gestores de descarga, etc.)

Pruebas detalladas para red de alta gerencia

- Validar que el nombre de la WLAN pueda ser cambiada (RG-02) por RG-11 y validar se mantengan las configuraciones establecidas en la Consola según lineamientos definidos
- Validar ingreso de equipo con Mac address registrada (en la Consola)
- Validar ingreso de equipo con Mac address no registrada (en la Consola)
- Validar ingreso de pre frase correcta, validar logs, status
- Validar ingreso de pre frase incorrecta, validar logs, status

- Validar direccionamiento provisto por medio de DHCP de Servidor Windows 2008, verificar en DHCP de Windows
- Validar ingreso de credenciales de Active Directory y aplicación de políticas de usuario con usuario y clave correcta, en especial validar usuario posea configuración por defecto y sin posibilidad de edición del proxy interno
- Validar ingreso de credenciales de Active Directory y aplicación de políticas de usuario con usuario y/o clave incorrecta
- Validar desde varios dispositivos que el SSID no pueda ser visualizado
- Validar con usuario y clave correcta y una vez logueado el usuario de Active Directory no solicite el ingreso de clave al menos por dos horas
- Verificar en la Consola de administración exista rastros del equipo adicionado a la WLAN
- Verificar que la red WLAN este solo disponible entre las 08:00 a 22:00
- Verificar el AB disponible para la red (10 Mbps Subida y 12 Mbps de bajada)
- Acceder a la WLAN con 5 diferentes usuarios y efectuar peticiones hacia varios tipos de contenidos, verificar se ejecute balanceo de carga entre los usuarios
- Verificar no exista conectividad hacia otras WLANs
- Verificar no exista conectividad y vista de otros clientes de las misma WLAN
- Validar conectividad hacia equipos de la red interna (según equipos colocados en políticas)
- Validar restricción de acceso por medio de proxy y bajo privilegios de usuario

Pruebas detalladas para red clientes y proveedores

- Validar que el nombre de la WLAN pueda ser cambiada (RG-03) por RG-12 y validar se mantengan las configuraciones establecidas en la Consola según lineamientos definidos
- Validar ingreso de pre frase correcta, validar logs, status
- Validar ingreso de pre frase incorrecta, validar logs, status
- Validar direccionamiento IP provisto por medio Zone Director
- Validar acceso de tipo guest Access con clave de acceso correcta
- Validar acceso de tipo guest Access con clave de acceso incorrecta
- Validar no exista acceso de tipo guest Access con clave de acceso correcta desde más de un equipo
- Validar mensaje de términos de uso y aceptación de acceso a la red
- Validar desde varios dispositivos que el SSID no pueda ser visualizado
- Verificar en la Consola de administración exista rastros del equipo adicionado a la WLAN
- Verificar que la red WLAN este solo disponible entre las 08:00 a 22:00
- Verificar el AB disponible para la red (2 Mbps Subida y 1 Mbps de bajada)
- Acceder a la WLAN con 5 diferentes usuarios y efectuar peticiones hacia varios tipos de contenidos, verificar se ejecute balanceo de carga entre los usuarios
- Validar no exista conectividad hacia equipo alguno de la red interna (prueba crítica)
- Verificar no exista conectividad hacia otras WLANs
- Verificar no exista conectividad y vista de otros clientes de las misma WLAN
- Validar restricción de acceso a sitios prohibidos (PSP, Pornografía, Gestores de descarga, etc.) y limitaciones adicionales

Pruebas detalladas para red equipos celulares

- Validar que el nombre de la WLAN pueda ser cambiada (RG-04) por RG-13 y validar se mantengan las configuraciones establecidas en la Consola según lineamientos definidos
- Validar ingreso de pre frase correcta, validar logs, status
- Validar ingreso de pre frase incorrecta, validar logs, status
- Validar correcto registro desde equipo con mac address existente en Consola
- Validar registro desde equipo con mac address no existente en Consola e imposibilidad de acceso
- Validar direccionamiento IP provisto por medio Zone Director
- Validar desde varios dispositivos que el SSID no pueda ser visualizado
- Verificar en la Consola de administración exista rastros del equipo adicionado a la WLAN
- Verificar que la red WLAN este solo disponible entre las 08:00 a 22:00
- Verificar el AB disponible para la red (2 Mbps Subida y 1 Mbps de bajada)
- Acceder a la WLAN con 5 diferentes usuarios y efectuar peticiones hacia varios tipos de contenidos, verificar se ejecute balanceo de carga entre los usuarios
- Validar no exista conectividad hacia equipo alguno de la red interna (prueba crítica)
- Verificar no exista conectividad hacia otras WLANs
- Verificar no exista conectividad y vista de otros clientes de las misma WLAN
- Validar restricción de acceso a sitios prohibidos (PSP, Pornografía, Gestores de descarga, etc.) y limitaciones adicionales

Pruebas a realizar desde Consola

- Simular desconexión o inhabilitación de Consola de administración y validar funcionalidad de las WLANs
- Conectar un nuevo AP y verificar el mismo no sea adicionado a la Consola de administración
- Verificar exista restricción de 20 clientes por AP
- Verificar exista logs de toda mac address ingresada y clave de tipo guest Access ingresada
- Eliminar la mac address de un equipo y clave tipo guest Access ingresada y verificar no exista accesos a la WLAN correspondiente

Pruebas adicionales

- Verificar monitoreo desde herramientas de monitoreo SNMP
- Verificar en equipos internos no exista peticiones desde Red 192.168.103.0/24
- Verificar reglas de denegación de servicios para la red 192.168.103.0/24 desde toda red interna

Documento Plan de implementación y roll back hacia ambiente de test (o pre producción)

Consta en el presente documento el detalle de cambios a considerar para el paso de la presente solución de ambiente de desarrollo a test. Contempla cambios a ejecutarse en equipos ya existentes así como en equipos provistos de la nueva solución.

Cambios a nivel de Router

Previo al cambio

Acceder al equipo (10.0.200.1) y obtener respaldo de configuración del equipo.

Cambio a considerar

ip route 192.168.100.0 255.255.255.0 10.0.207.100

Plan de roll back

No ip route 192.168.100.0 255.255.255.0 10.0.207.100

Cambios a nivel de switch de distribución

No aplica

Cambios a nivel de switches de acceso

Previo al cambio

Acceder a equipos (10.0.207.16, 10.0.207.19, 10.0.207.21, 10.0.207.24, 10.0.207.27, 10.0.207.30, 10.0.207.33, 10.0.207.36, 10.0.207.39, 10.0.207.41) y obtener respaldo de configuración del equipo.

Cambio a considerar

Configurar puerto 23 con acceso a Vlan113

Plan de roll back

Configurar puerto 23 con acceso a Vlan112 y/o aplicar respaldo

Cambios a nivel de firewall externo

Nuevas rutas

Previo al cambio

Acceder a cada nodo del firewall externo: equipos (10.0.201.3, 10.0.201.2) y obtener imagen de rutas existentes

Cambio a considerar

Configurar ruta a subred 192.168.100.0/24

Plan de roll back

Eliminar ruta creada

Nuevas reglas, objetos

Previo al cambio

1. Buscar la regla navegación wireless y verificar configuraciones
2. Buscar regla Servicios de administración y obtener respaldo de configuraciones existentes
3. Buscar regla ICMP monitoreo y obtener respaldo de las configuraciones

Cambio a considerar

1. Agregar al Grupo LAN_Fijas un nuevo objeto para la sub 192.168.100.0/24
2. Agregar objetos correspondientes a los nuevos equipos e incorporarlos al grupo G_Admin_Servicios
3. Agregar objetos correspondientes a los nuevos equipos e incorporarlos a los grupos G_ICMP Operadores e ICMP_Servidores

Plan de roll back

1. Eliminar objeto creado para subred 192.168.100.0/24
2. Eliminar objetos del grupo G_Admin_Servicios
3. Eliminar objetos de grupos G_ICMP Operadores e ICMP_Servidores

Cambios a nivel de firewall interno

Previo al cambio

Acceder a reglas de firewall y ubicar regla: red inalámbrica, obtener detalle de configuraciones existentes

Cambio a considerar

Agregar subred 192.168.100.0/24 en Regla: red inalámbrica

Plan de roll back

Eliminar subred 192.168.100.0/24 en Regla: red inalámbrica

Cambios a nivel de Servidor Windows 2008 R2

Previo al cambio

Identificar status de rol DHCP, de existir configuraciones guardar un respaldo

Cambio a considerar

Colocar configuraciones para direccionamiento DHCP desde subred 192.168.100.0/24

Plan de roll back

Eliminar configuraciones colocadas

Cambios a nivel de proxy Fore Front TMG

Previo al cambio

Validar si dentro del adaptador de red consta la subred 192.168.100/24

Cambio a considerar

Configurar subred 192.168.100/24

Plan de roll back

Eliminar configuraciones colocadas

Cambios a nivel de Sites de Active Directory

Previo al cambio

Validar si dentro de las subredes existentes en Sites consta la subred 192.168.100/24

Cambio a considerar

Configurar subred 192.168.100/24

Plan de roll back

Eliminar subred 192.168.100/24

Cambios a nivel de Zone Director

Previo al cambio

Obtener respaldo de imagen de configuraciones existentes en equipo Zone Director

Cambio a considerar

Colocar la IP del equipo Zone Director bajo direccionamiento de la subred de Pruebas, para el caso con IP 192.168.100.100. Verificar el nombre del equipo conste con el formato: Adm_Mat_AP01.

En la opción policy list (lista de accesos de equipos permitidos desde WLAN RG02), eliminar los equipos existentes y colocar los siguientes, tabla 35:

Tabla 35. Detalle de servidores test

IP	Nombre Equipo
10.0.201.10	UioMat-DC01
10.0.201.11	UioMat-Cor01
10.0.201.13	UioMat-Lyn01
10.0.201.42	UioMat-Pro01
10.0.201.60	UioMat-Ant01
192.168.100.10	PruMat-DC01
192.168.100.20	PruMat-Sha01
192.168.100.28	PruMat-IIS01

Fuente: (Erazo, 2016), Elaboración propia

Colocar la IP de cada AP en base al detalle de la subred de Pruebas, considerar las siguientes IPs, verificar nomenclatura en base a nombres definidos (suele perderse conectividad desde la consola, en cuyo caso se debe efectuar el cambio desde el AP).

- Adm_Mat_AP02 192.168.102.102 **AP a colocar en Piso 4**
- Adm_Mat_AP03 192.168.102.103 **AP a colocar en Piso 5**
- Adm_Mat_AP04 192.168.102.104 **AP a colocar en Piso 6**
- Adm_Mat_AP05 192.168.102.105 **AP a colocar en Piso 7**
- Adm_Mat_AP06 192.168.102.106 **AP a colocar en Piso 8**

- Adm_Mat_AP07 192.168.102.107 **AP a colocar en Piso 9**
- Adm_Mat_AP08 192.168.102.108 **AP a colocar en Piso 10**
- Adm_Mat_AP09 192.168.102.109 **AP a colocar en Piso 11**
- Adm_Mat_AP10 192.168.102.110 **AP a colocar en Piso 12**

Configurar DHCP

Confirmar se encuentre configurado el rango 192.168.103.5 al192.168.103.250 (configuración pre existente)

Plan de roll back

Aplicar imagen de respaldo en equipo Zone Director

Fase de Pruebas

Documento resultado de pruebas

Pruebas detalladas para red de alta gerencia

- **Validar que el nombre de la WLAN pueda ser cambiada (RG-01) por RG-10 y validar se mantengan las configuraciones establecidas en la Consola según lineamientos definidos**

  El cambio del ESSID no influye en las configuraciones ya existentes, las mismas se mantienen. Es fundamental considerar en el despliegue a producción los nombres finales para los ESSIDs

- **Validar ingreso de equipo con Mac address registrada (en la Consola)**

  Se valida el normal acceso toda vez que se cumple con el ingreso de la pre frase y del usuario de Active Directory. Se evidencia desde la Consola de administración el registro

del usuario conectado, del nombre del equipo desde el cual ingresó, el log de las peticiones efectuadas desde el equipo, el uso de AB y el AP al cual está conectado

- **Validar ingreso de equipo con Mac address no registrada (en la Consola)**

  Se valida la imposibilidad de accesos desde un equipo cuya mac address no está incluida en la consola de administración. Ya que se coloca la pre frase correcta se logra visualizar el log de acceso a la WLAN desde la consola, a su vez se valida el no tener accesos correcto al no estar registrada la mac address

- **Validar ingreso de pre frase correcta, validar logs, status**

  Al colocar la pre frase se logra validar el log de acceso desde la consola de administración sea esta o no correcta respecto a autenticación por mac addrees o Active Directory

- **Validar ingreso de pre frase incorrecta, validar logs, status**

  Al colocar la pre frase incorrecta se identifica log desde la consola

- **Validar direccionamiento provisto por medio de DHCP de Servidor Windows 2008, verificar en DHCP de Windows**

  El/los equipo(s) conectado(s) a la WLAN se encuentran registrados en el rol de DHCP de Windows 2008 R2

- **Validar ingreso de credenciales de Active Directory y aplicación de políticas de usuario con usuario y clave correcta**

  Se valida la autenticación por medio de Active Directory y la correcta inclusión de políticas de usuario.

- **Validar ingreso de credenciales de Active Directory y aplicación de políticas de usuario con usuario y/o clave incorrecta**

Se ejecuta validación con combinaciones (usuario activo con clave incorrecta, usuario y clave incorrecta) en ambos casos el mensaje indica el texto **usuario o clave incorrectos**. Es fundamental el acotar que es requerido colocar el dominio al que corresponde junto con el usuario; acepta los formatos (dominio\nombre_usuario o usuario@dominio). Este tema debe ser clarificado en las capacitaciones a usuarios finales

- **Validar desde varios dispositivos que el ESSID no pueda ser visualizado**

  Se verifica tener el ESSID en modo oculto

- **Validar con usuario y clave correcta y una vez logueado el usuario de Active Directory no solicite el ingreso de clave al menos por dos horas**

  Se verifica que de tener el equipo abierto (pantalla abierta), solo solicita la autenticación propia del equipo y al ingresarla correctamente simula conectividad similar a la obtenida en red cableada (prueba ejecutada con validación de 4 horas). Se acota que de tener el equipo bloqueado (pantalla cerrada) si solicita autenticación (autenticación de Directorio Activo)

- **Verificar en la Consola de administración exista rastros del equipo adicionado a la WLAN**

  Toda autenticación mantiene logs de las actividades de los usuarios finales y permite desconexión forzada en caso de requerir (Ej. Alto consumo de AB)

- **Verificar que la red WLAN este solo disponible entre las 08:00 a 22:00**

  De intentar conexiones en horarios previo o después del período establecido no permite acceso (simula status de red WLAN inexistente o no alcanzable desde la ubicación geográfica)

- **Verificar el AB disponible para la red (10 Mbps Subida y 12 Mbps de bajada)**

  Al efectuar una validación con un solo usuario conectado se verifica el alcanzar los umbrales expuestos, se valida desde varias ubicaciones de un mismo piso

- **Acceder a la WLAN con 5 diferentes usuarios y efectuar peticiones hacia varios tipos de contenidos, verificar se ejecute balanceo de carga entre los usuarios**

  Al realizar esta simulación de carga con 5 usuarios se identifica el dividir el AB entre los usuarios conectados de forma simétrica, se valida incluso que al tener visibilidad desde el AP del equipo inferior o superior y según validaciones propias del equipo realiza el balanceo de tal forma que haya similar número de usuarios por AP. Se verifica existir configuraciones automáticas para selección de canal, provisión de servicio por medio de un determinado AP

- **Validar conectividad hacia equipos de la red interna (experiencia de usuario similar a la existente al estar conecta de forma alámbrica)**

  Se valida normal acceso a los equipos y servicios provisto en la red interna de datos en base a los privilegios que posea el usuario. Se valida normal conectividad a los sitios validados, se efectúan pruebas de impresión de documentos, acceso a SFTPs, Intranet, correo, consola de antivirus, Lync

- **Verificar no exista conectividad hacia otras WLANs**

  Desde la WLAN no se puede visualizar equipos de las otras WLANs

- **Verificar no exista conectividad y vista de otros clientes de las misma WLAN**

  Los clientes que forman parte de la WLAN no poseen permiso ICMP. Al usar software de rastreo de equipos solo se identifica el equipo local y su gateway

- **Validar restricción de acceso a sitios prohibidos (PSP, Pornografía, Gestores de descarga, etc.)**

  Se valida navegación hacia redes sociales, sitios permitidos desde red alámbrica (con similares resultados), a su vez se detecta restricciones y mensajes de prohibición hacia sitios peligrosos (según definiciones internas establecidas en firewall de salida Internet)

Pruebas detalladas para red usuarios con laptop

- **Validar que el nombre de la WLAN pueda ser cambiada (RG-02) por RG-11 y validar se mantengan las configuraciones establecidas en la Consola según lineamientos definidos**

  El cambio del ESSID no influye en las configuraciones ya existentes, las mismas se mantienen. Es fundamental considerar en el despliegue a producción los nombres finales para los ESSIDs

- **Validar ingreso de equipo con Mac address registrada (en la Consola)**

  Se valida el normal acceso toda vez que se cumple con el ingreso de la pre frase y del usuario de Active Directory. Se evidencia desde la Consola de administración el registro del usuario conectado, del nombre del equipo desde el cual ingresó, el log de las peticiones efectuadas desde el equipo, el uso de AB y el AP al cual está conectado

- **Validar ingreso de equipo con Mac address no registrada (en la Consola)**

  Se valida la imposibilidad de accesos desde un equipo cuya mac address no está incluida en la consola de administración. Ya que se coloca la pre frase correcta se logra visualizar el log de acceso a la WLAN desde la consola, a su vez se valida el no tener accesos correcto al no estar registrada la mac address

- **Validar ingreso de pre frase correcta, validar logs, status**

  Al colocar la pre frase se logra validar el log de acceso desde la consola de administración sea esta o no correcta respecto a autenticación por mac addrees o Active Directory

- **Validar ingreso de pre frase incorrecta, validar logs, status**

  Al colocar la pre frase incorrecta se identifica log desde la consola

- **Validar direccionamiento provisto por medio de DHCP de Servidor Windows 2008, verificar en DHCP de Windows**

  El/los equipo(s) conectado(s) a la WLAN se encuentran registrados en el rol de DHCP de Windows 2008 R2

- **Validar ingreso de credenciales de Active Directory y aplicación de políticas de usuario con usuario y clave correcta, en especial validar usuario posea configuración por defecto y sin posibilidad de edición del proxy interno**

  Se valida que al acceder con usuario correcto de Active Directory se ejecuten las políticas internas a nivel de usuario, en el presente caso imposibilita el poder realizar cambios en configuración de proxy. Loa accesos a Internet varían de acuerdo a las atribuciones que posee el usuario

- **Validar ingreso de credenciales de Active Directory y aplicación de políticas de usuario con usuario y/o clave incorrecta**

  Se ejecuta validación con combinaciones (usuario activo con clave incorrecta, usuario y clave incorrecta) en ambos casos el mensaje indica el texto **usuario o clave incorrectos**. Es fundamental el acotar que es requerido colocar el dominio al que corresponde junto

con el usuario; acepta los formatos (dominio\nombre_usuario o usuario@dominio). Este tema debe ser clarificado en las capacitaciones a usuarios finales

- **Validar desde varios dispositivos que el ESSID no pueda ser visualizado**

  Se verifica tener el ESSID en modo oculto

- **Validar con usuario y clave correcta y una vez logueado el usuario de Active Directory no solicite el ingreso de clave al menos por dos horas**

  Se verifica que de tener el equipo abierto (pantalla abierta), solo solicita la autenticación propia del equipo y al ingresarla correctamente simula conectividad similar a la obtenida en red cableada (prueba ejecutada con validación de 4 horas). Se acota que de tener el equipo bloqueado (pantalla cerrada) si solicita autenticación (autenticación de Directorio Activo)

- **Verificar en la Consola de administración exista rastros del equipo adicionado a la WLAN**

  Toda autenticación mantiene logs de las actividades de los usuarios finales y permite desconexión forzada en caso de requerir (Ej. Alto consumo de AB)

- **Verificar que la red WLAN este solo disponible entre las 08:00 a 22:00**

  De intentar conexiones en horarios previo o después del período establecido no permite acceso (simula status de red WLAN inexistente o no alcanzable desde la ubicación geográfica)

- **Verificar el AB disponible para la red (4 Mbps Subida y 4 Mbps de bajada)**

  Al efectuar una validación con un solo usuario conectado se verifica el alcanzar los umbrales expuestos, se valida desde varias ubicaciones de un mismo piso

- **Acceder a la WLAN con 5 diferentes usuarios y efectuar peticiones hacia varios tipos de contenidos, verificar se ejecute balanceo de carga entre los usuarios**

  Al realizar esta simulación de carga con 5 usuarios se identifica el dividir el AB entre los usuarios conectados de forma simétrica, se valida incluso que al tener visibilidad desde el AP del equipo inferior o superior y según validaciones propias del equipo realiza el balanceo de tal forma que haya similar número de usuarios por AP. Se verifica existir configuraciones automáticas para selección de canal, provisión de servicio por medio de un determinado AP.

- **Validar conectividad hacia equipos de la red interna (según equipos colocados en políticas)**

  Se valida el tener accesos a los diferentes servicios provistos desde la red interna. Se constata no tener conectividad sino a equipos incluidos en listado de políticas de Zone Director.

- **Validar restricción de acceso por medio de proxy y bajo privilegios de usuario**

  La provisión de Internet se genera por medio del proxy existente y bajo los privilegios que posea el usuario en el aplicativo Forefront. Se valida accesos a Intranet y herramienta de control de solicitudes sin presentarse problema alguno.

Pruebas detalladas para red clientes y proveedores

- **Validar que el nombre de la WLAN pueda ser cambiada (RG-03) por RG-12 y validar se mantengan las configuraciones establecidas en la Consola según lineamientos definidos**

El cambio del ESSID no influye en las configuraciones ya existentes, las mismas se mantienen. Es fundamental considerar en el despliegue a producción los nombres finales para los ESSIDs

- **Validar ingreso de pre frase correcta, validar logs, status**

  Al colocar la pre frase se logra validar el log de acceso desde la consola de administración sea esta o no correcta respecto a autenticación por mac addrees o Active Directory

- **Validar ingreso de pre frase incorrecta, validar logs, status**

  Al colocar la pre frase incorrecta se identifica log desde la consola

- **Validar acceso de tipo guest Access con clave de acceso correcta**

  Para obtener pantalla de validación de acceso guest Access es requerido realizar una petición desde el navegador, caso contario y si bien ya consta con direccionamiento IP no permite navegar, tema fundamental a ser aclarado en capacitaciones a usuarios. En cuanto a la prueba al colocar la clave temporal provista permite acceso a Internet

- **Validar acceso de tipo guest Access con clave de acceso incorrecta**

  Al desplegarse la pantalla de autenticación guest Access y de colocar una clave incorrecta emite error de **acceso denegado**. Se valida la página desplegada para acceso de clave de tipo guest accesss sea de tipo **https**

- **Validar no exista acceso de tipo guest Access con clave de acceso correcta desde más de un equipo**

  Al colocar una misma clave generada desde un segundo dispositivo emite error de denegación **clave en uso**

- **Validar direccionamiento IP provisto por medio Zone Director**

Se identifica tener una IP correspondiente a la subred 192.168.103.0/24

- **Validar mensaje de términos de uso y aceptación de acceso a la red**

  Una vez ingresada la clave emite una pantalla de aceptación de términos de uso y aceptación

- **Validar desde varios dispositivos que el ESSID no pueda ser visualizado**

  Se verifica tener el ESSID en modo oculto

- **Verificar en la Consola de administración exista rastros del equipo adicionado a la WLAN**

  Toda autenticación mantiene logs de las actividades de los usuarios finales y permite desconexión forzada en caso de requerir (Ej. Alto consumo de AB)

- **Verificar que la red WLAN este solo disponible entre las 08:00 a 22:00**

  De intentar conexiones en horarios previo o después del período establecido no permite acceso (simula status de red WLAN inexistente o no alcanzable desde la ubicación geográfica)

- **Verificar el AB disponible para la red (2 Mbps Subida y 1 Mbps de bajada)**

  Al efectuar una validación con un solo usuario conectado se verifica el alcanzar los umbrales expuestos, se valida desde varias ubicaciones de un mismo piso

- **Acceder a la WLAN con 5 diferentes usuarios y efectuar peticiones hacia varios tipos de contenidos, verificar se ejecute balanceo de carga entre los usuarios**

  Al realizar esta simulación de carga con 5 usuarios se identifica el dividir el AB entre los usuarios conectados de forma simétrica, se valida incluso que al tener visibilidad desde el AP del equipo inferior o superior y según validaciones propias del equipo realiza el balanceo de tal forma que haya similar número de usuarios por AP. Se verifica existir

configuraciones automáticas para selección de canal, provisión de servicio por medio de un determinado AP

- **Validar no exista conectividad hacia equipo alguno de la red interna (prueba crítica)**

  Se efectúa validaciones desde el equipo de usuario final sin poder tener accesos a equipos de la red interna. Se efectúa validaciones de logs de reglas de denegación existentes en firewall de redes internas más no se detecta hit alguno de intentos de conexión desde algún equipo de la subred 192.168.103.0/24. Si bien los resultados son los esperados se recomienda ejecutar pruebas adicionales respecto a este tema

- **Verificar no exista conectividad hacia otras WLANs**

  Desde la WLAN no se puede visualizar equipos de las otras WLANs

- **Verificar no exista conectividad y vista de otros clientes de las misma WLAN**

  Los clientes que forman parte de la WLAN no poseen permiso ICMP. Al usar software de rastreo de equipos solo se identifica el equipo local y su gateway

- **Validar restricción de acceso a sitios prohibidos (PSP, Pornografía, Gestores de descarga, etc.) y limitaciones adicionales**

  Se deniega peticiones de acceso a sitios prohibidos y demás restricciones colocadas en el equipo de administración, adicional a restricciones propias del equipo firewall de salida a Internet (bajo consideraciones establecidas para todo origen)

Pruebas detalladas para red equipos celulares

- **Validar que el nombre de la WLAN pueda ser cambiada (RG-04) por RG-13 y validar se mantengan las configuraciones establecidas en la Consola según lineamientos definidos**

El cambio del ESSID no influye en las configuraciones ya existentes, las mismas se mantienen. Es fundamental considerar en el despliegue a producción los nombres finales para los ESSIDs

- **Validar ingreso de pre frase correcta, validar logs, status**

  Al colocar la pre frase se logra validar el log de acceso desde la consola de administración sea esta o no correcta respecto a autenticación por mac addrees o Active Directory

- **Validar ingreso de pre frase incorrecta, validar logs, status**

  Al colocar la pre frase incorrecta se identifica log desde la consola

- **Validar ingreso de equipo con Mac address registrada (en la Consola)**

  Se valida el normal acceso toda vez que se cumple con el ingreso de la pre frase y del usuario de Active Directory. Se evidencia desde la Consola de administración el registro del usuario conectado, del nombre del equipo desde el cual ingresó, el log de las peticiones efectuadas desde el equipo, el uso de AB y el AP al cual está conectado

- **Validar ingreso de equipo con Mac address no registrada (en la Consola)**

  Se valida la imposibilidad de accesos desde un equipo cuya mac address no está incluida en la consola de administración. Ya que se coloca la pre frase correcta se logra visualizar el log de acceso a la WLAN desde la consola, a su vez se valida el no tener accesos correcto al no estar registrada la mac address

- **Validar direccionamiento IP provisto por medio Zone Director**

  Se identifica tener una IP correspondiente a la subred 192.168.103.0/24

- **Validar desde varios dispositivos que el ESSID no pueda ser visualizado**

  Se verifica tener el ESSID en modo oculto

- **Verificar en la Consola de administración exista rastros del equipo adicionado a la WLAN**

  Toda autenticación mantiene logs de las actividades de los usuarios finales y permite desconexión forzada en caso de requerir (Ej. Alto consumo de AB)

- **Verificar que la red WLAN este solo disponible entre las 08:00 a 22:00**

  De intentar conexiones en horarios previo o después del período establecido no permite acceso (simula status de red WLAN inexistente o no alcanzable desde la ubicación geográfica)

- **Verificar el AB disponible para la red (2 Mbps Subida y 1 Mbps de bajada)**

  Al efectuar una validación con un solo usuario conectado se verifica el alcanzar los umbrales expuestos, se valida desde varias ubicaciones de un mismo piso

- **Acceder a la WLAN con 5 diferentes usuarios y efectuar peticiones hacia varios tipos de contenidos, verificar se ejecute balanceo de carga entre los usuarios**

  Al realizar esta simulación de carga con 5 usuarios se identifica el dividir el AB entre los usuarios conectados de forma simétrica, se valida incluso que al tener visibilidad desde el AP del equipo inferior o superior y según validaciones propias del equipo realiza el balanceo de tal forma que haya similar número de usuarios por AP. Se verifica existir configuraciones automáticas para selección de canal, provisión de servicio por medio de un determinado AP

- **Validar no exista conectividad hacia equipo alguno de la red interna (prueba crítica)**

  Se efectúa validaciones desde el equipo de usuario final sin poder tener accesos a equipos de la red interna. Se efectúa validaciones de logs de reglas de denegación existentes en

firewall de redes internas más no se detecta hit alguno de intentos de conexión desde algún equipo de la subred 192.168.103.0/24. Si bien los resultados son los esperados se recomienda ejecutar pruebas adicionales respecto a este tema

- **Verificar no exista conectividad hacia otras WLANs**

  Desde la WLAN no se puede visualizar equipos de las otras WLANs

- **Verificar no exista conectividad y vista de otros clientes de las misma WLAN**

  Los clientes que forman parte de la WLAN no poseen permiso ICMP. Al usar software de rastreo de equipos solo se identifica el equipo local y su gateway

- **Validar restricción de acceso a sitios prohibidos (PSP, Pornografía, Gestores de descarga, etc.) y limitaciones adicionales**

  Se deniega peticiones de acceso a sitios prohibidos y demás restricciones colocadas en el equipo de administración, adicional a restricciones propias del equipo firewall de salida a Internet (bajo consideraciones establecidas para todo origen)

Pruebas a realizar desde Consola

- **Simular desconexión o inhabilitación de Consola de administración y validar funcionalidad de las WLANs**

  Se desconecta de la red a la Consola de administración y se verifica el poder tener acceso desde las diferentes WLANs. Cabe acotar que por obvias razones es imposible generar nuevos accesos de tipo guest Access mientras exista indisponibilidad de la Consola de administración. Se detecta adicionalmente problemas de despliegue de pantalla de autenticación de Active Directory, más se valida que los usuarios ya conectados no sufren desconexión alguna.

- **Conectar un nuevo AP y verificar el mismo no sea adicionado a la Consola de administración**

  Al conectar un nuevo equipo a la red el mismo no es identificado por la Consola de administración. Par atar este nuevo dispositivo se debe efectuar un proceso manual.

- **Verificar exista restricción de 20 clientes por AP**

  Se ejecuta prueba con 20 equipos conectados a un AP, al colocar el usuario 21 permite adicionarlo pero lo ata al AP del piso superior

- **Verificar exista logs de toda mac address ingresada y clave de tipo guest Access ingresada**

  Se identifica en la Consola de administración todas las mac address registradas así como toda petición guest Access creada. Se valida que al eliminar un dato desde la consola (mac address o guest access) se pierda conectividad desde el equipo final

- **Eliminar la mac address de un equipo y clave tipo guest Access ingresada y verificar no exista accesos a la WLAN correspondiente**

  Se valida que al eliminar un dato desde la consola (mac address o guest access) se pierda conectividad desde el equipo final

Pruebas adicionales

- **Verificar monitoreo desde herramientas de monitoreo SNMP**

  Se verifica tener normal acceso desde herramientas internas

- **Verificar en equipos internos no exista peticiones desde red 192.168.103.0/24**

  No se registra peticiones en regla de denegación existente firewall interno (regla tiene registro de hits en valor 0)

- **Verificar reglas de denegación de servicios para la red 192.168.103.0/24 desde toda Red interna**

  Se han colocado algunas consideraciones para la red externa 192.168.103.0/24 a pesar de no haber conectividad hacia la red interna

Documento Plan de implementación y roll back hacia ambiente de producción

Consta en el presente documento el detalle de cambios a considerar para el paso de la presente solución de ambiente de test a producción. Contempla cambios a ejecutarse en equipos ya existentes así como en equipos provistos de la nueva solución.

Cambios a nivel de Router

Previo al cambio

Acceder al equipo (10.0.200.1) y obtener respaldo de configuración del equipo.

Cambio a considerar

interface GigabitEthernet0/1

ip address 10.0.212.0 255.255.255.0 secondary

Plan de roll back

interface GigabitEthernet0/1

no ip address 10.0.212.0 255.255.255.0 secondary

Cambios a nivel de switch de distribución

No aplica

Cambios a nivel de switches de acceso

Previo al cambio

Acceder a equipos (10.0.207.16, 10.0.207.19, 10.0.207.21, 10.0.207.24, 10.0.207.27, 10.0.207.30, 10.0.207.33, 10.0.207.36, 10.0.207.39, 10.0.207.41) y obtener respaldo de configuración del equipo.

Cambio a considerar

Configurar puerto 23 con acceso a Vlan1

Plan de roll back

Configurar puerto 23 con acceso a Vlan113 y/o aplicar respaldo

Cambios a nivel de firewall externo

Nuevas rutas

Previo al cambio

Acceder a cada nodo del firewall externo: equipos (10.0.201.3, 10.0.201.2) y obtener imagen de rutas existentes

Cambio a considerar

Configurar ruta a subred 10.0.212.0/24

Plan de roll back

Eliminar ruta creada

Nuevas reglas, objetos

Previo al cambio

1. Buscar la regla navegación wireless y verificar configuraciones
2. Buscar regla Servicios de administración y obtener respaldo de configuraciones existentes
3. Buscar regla ICMP monitoreo y obtener respaldo de las configuraciones

Cambio a considerar

1. Agregar al Grupo LAN_Fijas un nuevo objeto para la subred 10.0.212./24
2. Agregar objetos correspondientes a los nuevos equipos e incorporarlos al grupo G_Admin_Servicios
3. Agregar objetos correspondientes a los nuevos equipos e incorporarlos a los grupos G_ICMP Operadores e ICMP_Servidores

Plan de roll back

4. Eliminar objeto creado para subred 10.0.212./24

1. Eliminar objetos del grupo G_Admin_Servicios
2. Eliminar objetos de grupos G_ICMP Operadores e ICMP_Servidores

Cambios a nivel de firewall interno

Previo al cambio

Acceder a reglas de firewall y ubicar regla: red inalámbrica, obtener detalle de configuraciones existentes

Cambio a considerar

Agregar subred 10.0.212.0/24 en Regla: red inalámbrica

Plan de roll back

Eliminar subred 10.0.212.0/24 en Regla: red inalámbrica

Cambios a nivel de Servidor Windows 2008 R2

Previo al cambio

Identificar status de rol DHCP, de existir configuraciones guardar un respaldo

Cambio a considerar

Colocar configuraciones para direccionamiento DHCP desde subred 10.0.212.0/24

Plan de roll back

Eliminar configuraciones colocadas

Cambios a nivel de proxy ForeFront TMG

Previo al cambio

Validar si dentro del adaptador de red consta la subred 10.0.212.0/24

Cambio a considerar

Configurar subred 10.0.212.0/24

Plan de roll back

Eliminar configuraciones colocadas

Cambios a nivel de Sites de Active Directory

Previo al cambio

Validar si dentro de las subredes existentes en Sites consta la subred 10.0.212.0/24

Cambio a considerar

Configurar subred 10.0.212.0/24

Plan de roll back

Eliminar subred 10.0.212.0/24

Cambios a nivel de Zone Director

Previo al cambio

Obtener respaldo de imagen de configuraciones existentes en equipo Zone Director

Cambio a considerar

Colocar la IP del equipo Zone Director bajo direccionamiento de la subred de producción, para el caso con IP 10.0.212.230/24. Verificar el nombre del equipo conste con el formato: Adm_Mat_Wifi

En la opción policy list (lista de accesos de equipos permitidos desde WLAN RG02), eliminar los equipos existentes y colocar los siguientes, tabla 36:

Tabla 36. Detalle servidores producción

IP	Nombre Equipo
10.0.201.10	UioMat-DC01
10.0.201.11	UioMat-Cor01
10.0.201.13	UioMat-Lyn01
10.0.201.20	UioMat-Sha01

10.0.201.28	UioMat-IIS01
10.0.201.42	UioMat-Pro01
10.0.201.60	UioMat-Ant01

Fuente: (Erazo, 2016), Elaboración propia

Colocar la IP de cada AP en base al detalle de la subred de producción, considerar las siguientes IPs, verificar nomenclatura en base a nombres definidos (suele perderse conectividad desde la consola, en cuyo caso se debe efectuar el cambio desde el AP).

- Adm_Mat_AP01 10.0.212.231 **AP a colocar en Piso 3**
- Adm_Mat_AP02 10.0.212.232 **AP a colocar en Piso 4**
- Adm_Mat_AP03 10.0.212.233 **AP a colocar en Piso 5**
- Adm_Mat_AP04 10.0.212.234 **AP a colocar en Piso 6**
- Adm_Mat_AP05 10.0.212.235 **AP a colocar en Piso 7**
- Adm_Mat_AP06 10.0.212.236 **AP a colocar en Piso 8**
- Adm_Mat_AP07 10.0.212.237 **AP a colocar en Piso 9**
- Adm_Mat_AP08 10.0.212.238 **AP a colocar en Piso 10**
- Adm_Mat_AP09 10.0.212.239 **AP a colocar en Piso 11**
- Adm_Mat_AP10 10.0.212.240 **AP a colocar en Piso 12**

Configurar DHCP

Confirmar se encuentre configurado el rango 10.0.212.5 al 10.0.212.225

Nomenclatura para redes WLAN

Cambiar los nombres de los ESSIDs y descripción de las WLANs en base a lo expuesto en tabla 37:

Tabla 37. Nomenclatura nombres WLANs y ESSIDs

Detalle de la WLAN	Ambiente desarrollo/test	Ambiente producción	Ocultar SSID
red alta Gerencia	RG-01	Codec_insur	Si
red líneas de supervisión	RG-02	Cotopaxi	Si
red clientes y proveedores	RG-03	Code_red	No
red equipos celulares	RG-04	iPad de Juan	No

Fuente: (Erazo, 2016), Elaboración propia

Nota: Ingresar detalle de Mac address de equipos inventariados en Consola de administración. A su vez crear usuarios para los diferentes roles (estas tareas deben ser delegadas al oficial de seguridades, a realizar en conjunto con Ejecutor de proyecto). Actividad contempla creación de usuarios para generadores de accesos tipo guest por piso.

Plan de roll back

Aplicar imagen de respaldo en equipo Zone Director

Fase de Implementación

Informe de resultados obtenidos

Se consideran los siguientes puntos:

Una vez ejecutada la implementación y logrando los resultados esperados se requiere:

- Regularizar Acta de ingreso de equipos nuevos al Data Center

- Configurar nuevos equipos en herramientas internas de monitoreo
- Mantener un archivo actualizado de inventario de mac address de equipos de usuarios internos
- Potenciar campañas de concientización de uso de red inalámbrica mediante emisión de política de seguridad interna, acceso a la información y confidencialidad de la información
- Mantener respaldos de documentos físicos emitidos para generación de clave de usuario final, ante posibles auditorias
- Crear documento de inclusión de mac address en consola de Administración, en formato similar al existente para reglas de firewall

Topología de red general

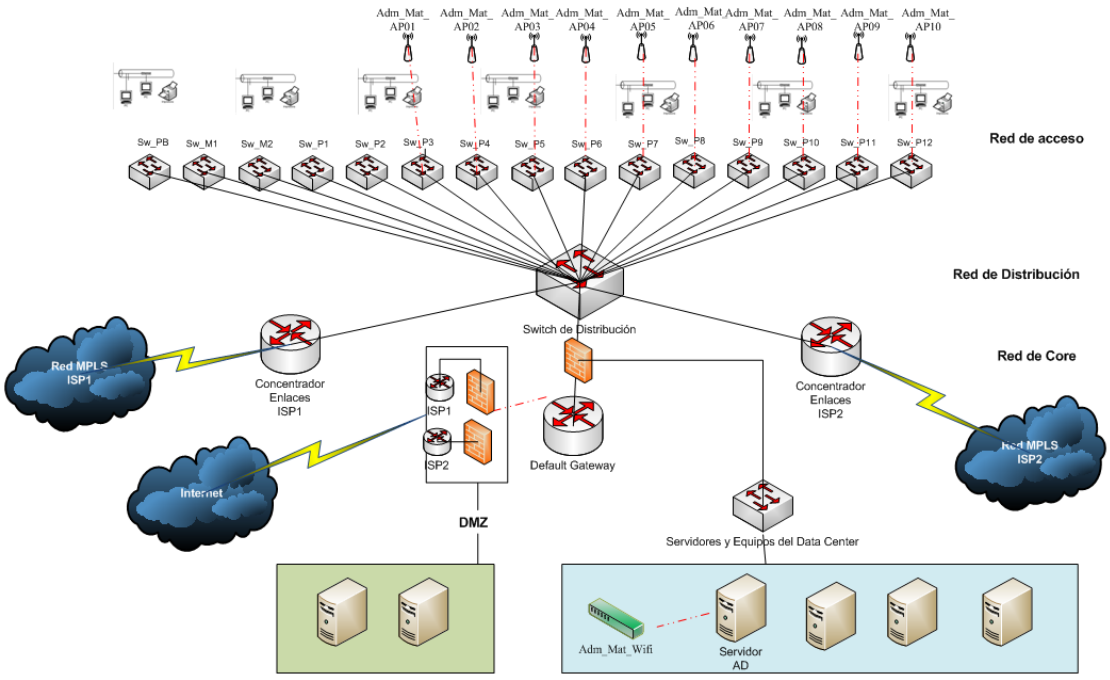

Figura 114. Topología de red general actualizada
Fuente: (Erazo 2016), Herramienta Visio, Elaboración propia

Fase de Post Implementación – Optimización

Acta de aceptación TI

Quito 21 de Octubre 2016

Por medio de la presente el área de redes y comunicaciones formaliza la entrega del proyecto "**Proyecto_Red_Inalambrica_Edf.Matriz**" al área de monitoreo y centro de cómputo. El proyecto ha realizado con éxito el desarrollo, pruebas e implementación de la solución que provee conectividad inalámbrica bajo lineamientos expuestos, incluye además la correcta formalización de ingreso de equipos hacia el Data Center. Se solicita su gentil validación y pruebas respecto a las herramientas de monitoreo, validación de temas de licenciamiento, entrega de equipos de backup, detalle de configuraciones y documentación actualizada del inventario de equipos.

En razón de lo antes expuesto el representante del área de monitoreo y centro de cómputo avalan la presente entrega, a su vez y bajo constancia de las actividades realizadas

Recibe

_____	_____
Ing. Daniel Rodas (Centro de cómputo)	Ing. Luis López (Sub gerente de tecnología)

Entrega

_____	_____
Ing. Juan Pablo Moreno (Ejecutor del Proyecto)	Ing. Daniel Rosero (Oficial de seguridades)
_____	_____
Ing. Pablo Tirado (Oficial de riesgos)	Ing. Marcelo Calderón (Soporte técnico/Pruebas)

Fase de nonitoreo y control

Documento definiciones de monitoreo de nueva solución

La solución implementada en el proyecto considera el acoplamiento de monitoreo mediante uso de SNMP. Se ha contemplado así las configuraciones requeridas en las diferentes herramientas de la institución.

El área de monitoreo y centro de cómputo ha definido las siguientes consideraciones para el monitoreo a realizarse de los equipos que conforman la solución:

- Alerta visual mediante herramientas Cacti, Whats Up, Visual Pulse
- Alerta visual/sonora mediante herramienta Pinger
- Envío de correos por medio de Whats Up y funcionalidad propia de la solución

Se acuerda el realizar un monitoreo permanente durante los horarios establecidos. Se establece que el seguimiento a problemas será validado directamente por el área de redes y comunicaciones.

Fase de Cierre

Acta formal de cierre

Quito 10 de Noviembre 2016

Por medio de la presente el área de tecnología de la institución formaliza la entrega y cierre del proyecto "**Proyecto_Red_Inalambrica_Edf.Matriz**". El proyecto ha realizado con éxito el desarrollo, pruebas, implementación y entrega formal al área de monitoreo y centro de cómputo incorporándose como un nuevo servicio provisto a la institución. En adelante la responsabilidad y mantenimiento forman parte del esquema normal y servicio provisto por dicha área. En razón de lo antes expuesto el representante del área de monitoreo y centro de

Cómputo así como el Representante del área de tecnología avalan la presente entrega, a su vez y bajo constancia de las actividades realizadas en las diferentes fases del proyecto. Adicionalmente consta la entrega y aceptación final por parte de proveedor en constancia de existir total acuerdo con la consecución de toda actividad referente a la compra de equipo, licenciamiento y demás por el provisto.

Recibe

_____

Dr. Juan Yépez (Sponsor)

Entrega

_____	_____
Ing. Daniel Rodas	Ing. Luis López
_____	_____
Ing. Rafael Mejía (Proveedor)	Ing. Daniel Coronel (Responsable de marketing)

4.4 Comparativa frente a la situación actual

Se había comentado al inicio del presente documento, que la institución si bien ejecuta proyectos de redes y comunicaciones los mismos se basan en plantillas de metodología MSF de donde la información resultante no brinda mayor detalle del cambio involucrado. A nivel general, el detalle de los 4 documentos existentes explica a nivel muy macro el objetivo esperado con el proyecto a implantar, el equipo a ser asignado al proyecto, los roles de los diferentes stakeholders, los entregables del producto a ser generado, la estrategia de comunicación de

avances, así como el detalle macro de necesidades a ser desarrolladas. En ninguno de los documentos existentes se contempla detalles de red como topología, status de salud actual, especificaciones técnicas, entre otros. En lo que respecta a dirección del proyecto como tal, no contempla oficialización alguna de documentación, mucho menos definición de responsabilidad de los ejecutores e intervinientes. Si bien las plantillas corresponden a una base de MSF el llenado de la información de dichos documentos no brinda mayor detalle de tema de costos, alcance, tiempos; mucho menos de temas de control de calidad. En el mejor de los casos se ha confirmado la existencia de estos 4 documentos en los repositorios del Portal documental interno: SharePoint, generando varias problemáticas:

- No se cuenta con información actualizada de los diagramas de red
- No se detalla documentación de cambios contemplados en el Diseño de la red
- No existe registros de los cambios efectuados en la red
- No existe detalle de equipos (costos, garantía de equipos, licenciamiento)

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Introducción

El presente capítulo expone un compendio de las definiciones finales identificadas, una vez ejecutado el caso de estudio.

5.1 Conclusiones

A lo largo del presente trabajo se efectuó un estudio y análisis comparativo de las metodologías de redes y a su vez respecto a metodologías de proyectos en general citadas por el autor. Se pudo identificar así que todas ellas realizan énfasis en el cumplimiento de objetivos técnicos y de negocio. Si bien existen diferencias en la profundidad con la cual se enfatiza algunos temas propios de proyecto, se ha propuesto una metodología que permita cubrir ambas necesidades.

Se identifica que toda metodología brinda lineamientos a ser desarrollados en las diferentes fases y basta información para su ejecución, más no provee plantillas que orienten a su generación.

Se ha ejecutado un caso de implementación real basado en la metodología propuesta por el autor cuyo objetivo es brindar una especificación detallada de los principales entregables que corresponden al diseño de red y a la provisión de nuevos servicios y cumplimiento de necesidades expuestas por el solicitante con fines de brindar una orientación de cómo elaborarlos.

La metodología propuesta por el autor brinda al ejecutor contemplar los siguientes objetivos:

- Acoplar escalabilidad a la red, permitiendo el adicionar nuevos equipos de comunicaciones, servicios y aplicaciones en consideración de mantener alta disponibilidad, gestión eficiente de la red y énfasis en temas de seguridad.
- Mantener un control de presupuesto asignado y ejecución del proyecto en base a lineamientos internos y en base a la metodología propuesta
- Mantener actualizada la información correspondiente al diseño de red y equipos que la conforman
- Efectuar actividades que permitan validar y verificar el estado de salud de la red previo acoplamiento de nuevas soluciones, considerando adicionalmente actualización y reemplazo de equipos (de requerir)
- Incorporar análisis de riesgos y aspectos de seguridad en toda actividad a ser realizada
- Contemplar en las diferentes soluciones el acoplamiento con políticas internas así como de entidades externas y entes regulatorios

Respecto a la aplicación de la metodología en la institución y en comparativa de la situación inicial, se pudo concluir que:

- La metodología propuesta se acopla a los objetivos de la organización respecto al cumplimiento de políticas y procedimientos internos a su vez aporta en el cumplimiento de objetivos propios del negocio
- Brindar aporte en generación de información a ser solicitada en auditorías internas y externas

A su vez brinda al área de tecnología los siguientes beneficios

- Mantener documentación actualizada de la red en cuanto a diagramas, inventario de equipo, puertos
- Permite prevenir requerimientos de provisión – reemplazo de equipos
- Aporta en la generación anual de presupuesto del área de tecnología
- Evidencia nuevos requerimientos, propuestas de mejora, puntos de fallo
- Formaliza nuevos requerimientos tales como: reglas de firewall, permisos o denegación de accesos

5.2 Recomendaciones

Se recomienda al ejecutor del proyecto tener una capacitación básica de manejo de proyectos a fin de contemplar al menos las 3 restricciones básicas: tiempo, costos, calidad y de preferencia tener control adicional sobre las 3 restricciones complementarias: alcance, recursos y riesgos. A su vez el cumplir los entregables propuestos o como mínimo el tener control sobre: un alcance bien delimitado, formalizar el acta de constitución del proyecto, definir un cronograma, formalizar cualquier cambio que no forme parte del plan inicial y formalizar el cierre del proyecto.

Es fundamental el mantener una base documental y de conocimientos donde consten todos los entregables del proyecto. Para el caso de la institución financiera y al existir un repositorio interno en SharePoint se recomienda el mantener en dicho aplicativo toda documentación del proyecto.

Es vital el tener un manejo de cronograma, siendo este posible llevarlo de diferentes maneras y bajo algunas herramientas disponibles en el mercado. Para el caso de la institución y

al tener un contrato especial con Microsoft; se recomienda el poder hacer uso de Microsoft Project Server, siendo idóneo el poder acoplarlo con SharePoint.

Se considera oportuno contar con un área especializada de Proyectos a fin de que permita brindar apoyo con los diferentes entregables de cada fase y realizar control del manejo de proyectos, en el caso de la institución financiera el apoyo y control del cumplimiento de la metodología propuesta puede ser manejada por el área de Procesos.

Se sugiere el mantener una correcta comunicación con todo el equipo del proyecto y generar reportes periódicos que permitan conocer el status del mismo.

Se recomienda el formalizar el cierre de cada fase y contar con la aprobación de los solicitantes de tal manera que se evite asunciones y posibles problemas.

Es vital el definir reuniones diarias con el equipo con fines de contemplar los avances y posibles obstáculos que se presenten en el desarrollo de las actividades

Se sugiere el realizar capacitaciones al usuario final previo a su implementación a su vez socializar el entregable o producto final teniendo énfasis en consideraciones de seguridad y cumplimiento de políticas internas.

REFERENCIAS Y BIBLIOGRAFIA

Lista de Referencias

[1] Beck K & Otros, *Manifiesto por el Desarrollo Ágil de Software*, recuperado de: http://agilemanifesto.org/iso/es/manifesto.html

[2] Garrido D, Ramírez J. *Implementación de una PMO en una empresa de Tecnología: Un análisis compartivo de metodologías de proyectos.* Recuperado de: http://www.umng.edu.co/documents/10162/745280/V3N1_8.pdf

[3] Mulcahi R, PMP, Otros (2013). *Preparación para el examen PMP®.* Estados Unidos de Norteamérica. RMC Publications, Inc.

[4] Oppenheimer P. (2010). *Top-Down Network Design, Third Edition*. Recuperado de: http://techbus.safaribooksonline.com/book/networking/9781587140051

[5] Orozco A. (2013). *Planos efectuados por SAT Comunicaciones*

[6] PMI®. (2016). *Qué es PMI.* Recuperado de: http://www.pmipr.org/page-1700183

[7] Schaffer G. (2009). *Project Management for Network Professionals*. Recuperado de http://www.cio.com/article/2431000/infrastructure/project-management-for-network-professionals.html

[8] Silvano F. Scrum y *métodos ágiles.* Recuperado de: http://es.slideshare.net/CLEFormacion/seminario-scrum-cleformacin

[9] Sholomon A, Kunath T. (2011). *Enterprise Network Testing: Testing Throughout the Network Lifecycle to Maximize Availability and Performance.* Recuperado de: http://techbus.safaribooksonline.com/book/networking/9781587140884

[10] Tapias D. (2014). *Ciclo de vida de los proyectos.* Recuperado de: http://arantxa.ii.uam.es/~proyectos/teoria/C4_Ciclo%20de%20vida.pdf

[11] Teare, D. (© 2008). *Designing for cisco internetwork solutions (desgn) (authorized ccda self-study guide) (exam 640-863), second edition.* Recuperado de: http://techbus.safaribooksonline.com/book/certification/ccda/9780132582407

[12] Wallace W. (2014), *Gestión de Proyectos*. Recuperado de: http://docslide.us/documents/gestion-de-proyectos-william-wallace.html

Bibliografía

[1] **Information Resources Management Association (IRMA)**, Networking and Telecommunications: Concepts, Methodologies, Tools and Applications, IGI Global, 2010, ISBN:9781605669861

[2] **Keith Hutton, Mark Schofield, Diane Teare,** Designing Cisco Network Service Architectures (ARCH) (Authorized Self-Study Guide)**,** Cisco Press, 2009, Second Edition, ISBN:9781587055744

[3] **Kim H. Pries and Jon M. Quigley**, Scrum Project Management, Auerbach Publications, 2011, ISBN:9781439825150

[4] Priscila Oppenheimer, Top-Down Network Design, Cisco Press, 2010, Third Edition, ISBN:9781587202834

[5] **Subramanian Chandramouli; Saikat Dutt,** PMI Agile Certified Practitioner —Excel with Ease, Pearson India, March 29, 2012, ISBN: 9788131773192